JOURNÉE DE L'INFONUAGIQUE

ISACA
Section de Québec

ATELIER DE FORMATION SUR LA CERTIFICATION CCSK

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE / CCSK

Hiver 2019

Tactika inc.

Qui suis-je ?

Clément Gagnon

- *clement.gagnon@tactika.com*
- Spécialiste en sécurité de l'information
  - + 30 ans d'expérience dans les TI
  - Entreprises : Tactika inc. et ID-M (en démarrage)
    - www.tactika.com
    - Id-m.me
  - Certifications : CISSP, CISA, CRISC, ISO2700x … CCSK,
  - Domaines d'intervention
    - Gestion des risques
    - Architecture haut niveau de sécurité et de réseautique
    - Infonuagique
      - Rédaction de stratégies et de cadres de référence pour des organismes gouvernementaux
      - Participer à l'implantation de services infonuagiques

Ce document

- Est un extrait du document de formation sur la sécurité de l'infonuagique pour l' obtention de la certification CCSK
  - Le document de formation s'inspire principalement du guide officiel de la Cloud Security Alliance « Security Guidance For Critical Areas of Focus in Cloud Computing v4.0 »
- N'est pas un remplacement du guide
- N'est pas approuvé par la Cloud Security Alliance / CSA

- Des informations complémentaires sont insérées dans ce document, elles sont marquées avec cette icone

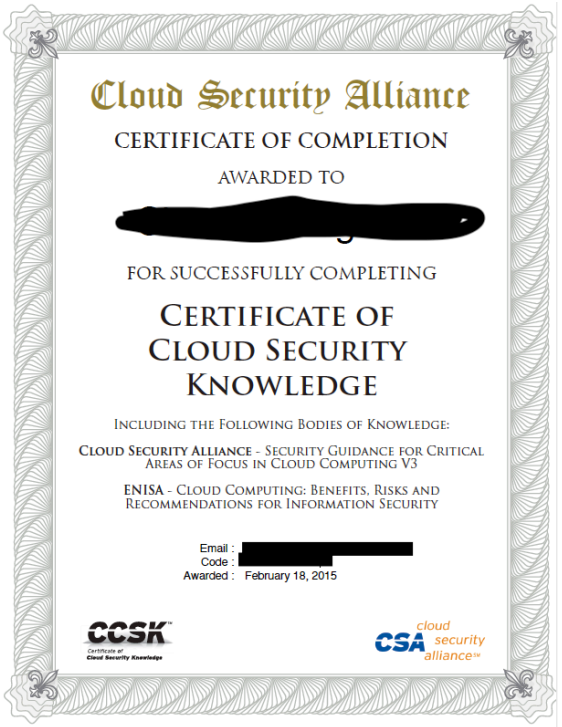
Liens importants

- **Document de formation**
  http://bit.ly/CCSK2019v2

- **Examens**
  http://bit.ly/ExamenCCSK2019-p1
  http://bit.ly/ExamenCCSK2019-p2

La certification *CERTIFICATE OF CLOUD SECURITY KNOWLEDGE /* CCSK

- Le CCSK est une certification sur la connaissance de la sécurité de l'information et de l'infonuagique
- Elle n'est pas associée à un fournisseur
- Il n'y a pas de date de fin de validité à cette certification
- Pour obtenir la certification
  - Étudier le corpus (peu importe le moyen)
  - S'inscrire et acheter le jeton d'examen sur le site du CSA
    https://ccsk.cloudsecurityalliance.org/
  - Réussir l'examen par Internet
- Examen
  - Durée: 90 minutes
  - 60 questions
  - Note de passage : 80 % (taux de réussite : 62%)
  - Livre ouvert
  - Coût : 395$US (jeton valide 2 ans)
  - Vous avez droit à 2 essais pour l'examen


Cloud Security Alliance

CERTIFICATE OF COMPLETION

AWARDED TO

[redacted]

FOR SUCCESSFULLY COMPLETING

CERTIFICATE OF CLOUD SECURITY KNOWLEDGE

INCLUDING THE FOLLOWING BODIES OF KNOWLEDGE:

CLOUD SECURITY ALLIANCE - SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3

ENISA - CLOUD COMPUTING: BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY

Email : [redacted]
Code : [redacted]
Awarded : February 18, 2015

CCSK Certificate of Cloud Security Knowledge

CSA cloud security alliance

La certification *CERTIFICATE OF CLOUD SECURITY KNOWLEDGE /* CCSK

- La certification CCSK est associée à un # de version
- La certification est basée sur la version 4 du « *Security Guidance For Critical Areas of Focus in Cloud Computing* » (octobre 2017)

CCSK et les autres certifications

- *Certificate of Cloud Security Knowledge* / CCSK
  - Création du *Cloud Security Alliance* / CSA
  - Contenu généraliste de nature tactique et stratégique, agnostique
  - 2 formats
    - CSSK Foundation (1 ou 2 jours)
    - CCSK PLUS (2 ou 3 jours, CSSK Foundation + laboratoire AWS ou Azure)

Sans péremption, Sans maintien de CPE, Coût unique

- ISACA
  - CISA, CRISC, CISM, etc.
- (ISC)2
  - CISSP, *Certified Cloud Security Professional* / CCSP
    - CSSP Création conjointe du (ISC)² et CSA mais géré par (ISC)²
    - *CCSP = CCSK + Expanded Governance Items + Traditional Security + Privacy + Data Center security*
    - Formation typique de 5 jours
    - Pas de lab, prérequis d'expérience de travail pour obtenir la certification
    - Examen se déroule dans un centre spécialisé, livre fermé

Avec péremption, Maintien de CPE, Coût unique + de maintien

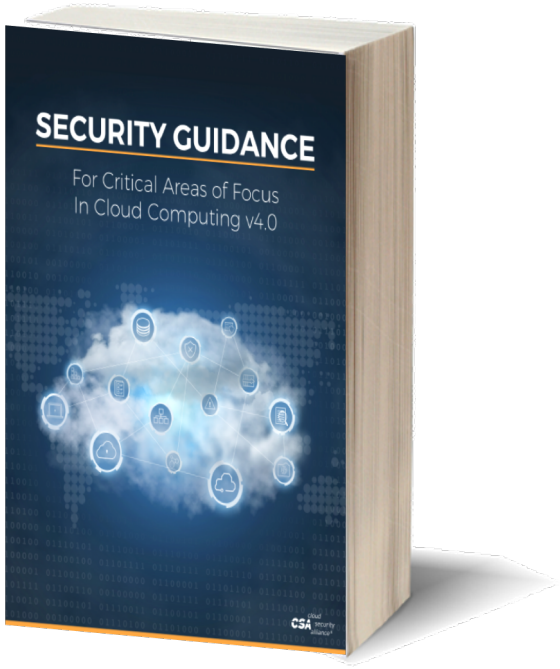
À venir, le CCAK !

- Expertise dans les audits de solutions de type infonuagique
- Basé sur les composants CCM, CAIQ et soutenir le programme STAR
- Sera disponible dans le troisième quart de 2020

Document principal de référence

Security Guidance
For Critical Areas of Focus in Cloud Computing
v4.0

https://cloudsecurityalliance.org/download/security-guidance-v4/



Deuxième document de référence

Cloud Computing, BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY

https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file

Autres documents de référence

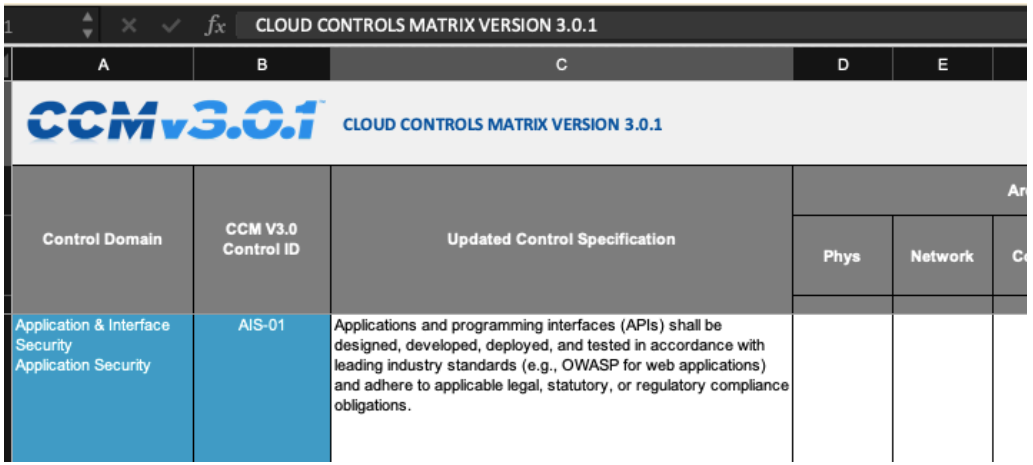
- **Cloud Control Matrix v3.0.1 / CCM**
  - Grille de correspondance des normes et pratiques recommandées pour l'infonuagique
    https://cloudsecurityalliance.org/group/cloud-controls-matrix/

- **Consensus Assessment Initiative Questionnaire v3.1 / CAIQ**
  - Auto-évaluation (*assessement*) sur les mesures de contrôle
    https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/

- **Programme *Security, Trust and Assurance Registry* / STAR**
  - STAR est une certification de confiance de l'industrie pour la sécurité des services cloud / Cloud Service Provider ou CSP
  - *CSA Open Certification Framework* (OCF) est un référenciel flexible, incrémentale et multicouche basé sur les directives de sécurité du CSA (prochaine planche)

Cloud Control Matrix v3.0.1 / CCM

- Cadre de conformité
- Chiffrier Excel
- 16 domaines
- 133 mesures de contrôle



CLOUD CONTROLS MATRIX VERSION 3.0.1

A	B	C	D	E
CCMv3.0.1	CLOUD CONTROLS MATRIX VERSION 3.0.1			
Control Domain	CCM V3.0 Control ID	Updated Control Specification	Ar	
			Phys	Network
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.		

- *ISO 27001/27002/27017/27018, NIST SP 800-53, AICPA TSC, ENISA Information Assurance Framework, German BSI C5, PCI DSS,, ISACA COBIT, NERC CIP*

Les domaines du CCSK et du CCM

CCSK

1. Cloud Computing Concepts and Architecture
2. Governance and Enterprise Risk Management
3. Legal Issues, Contracts and Electronic Discovery
4. Compliance and Audit Management
5. Information Governance
6. Management Plane and Business Continuity
7. Infrastructure Security
8. Virtualization and Containers
9. Incident Response
10. Application Security
11. Data Security and Encryption
12. Identity, Entitlement, and Access Management
13. Security as a Service
14. Related Technologies

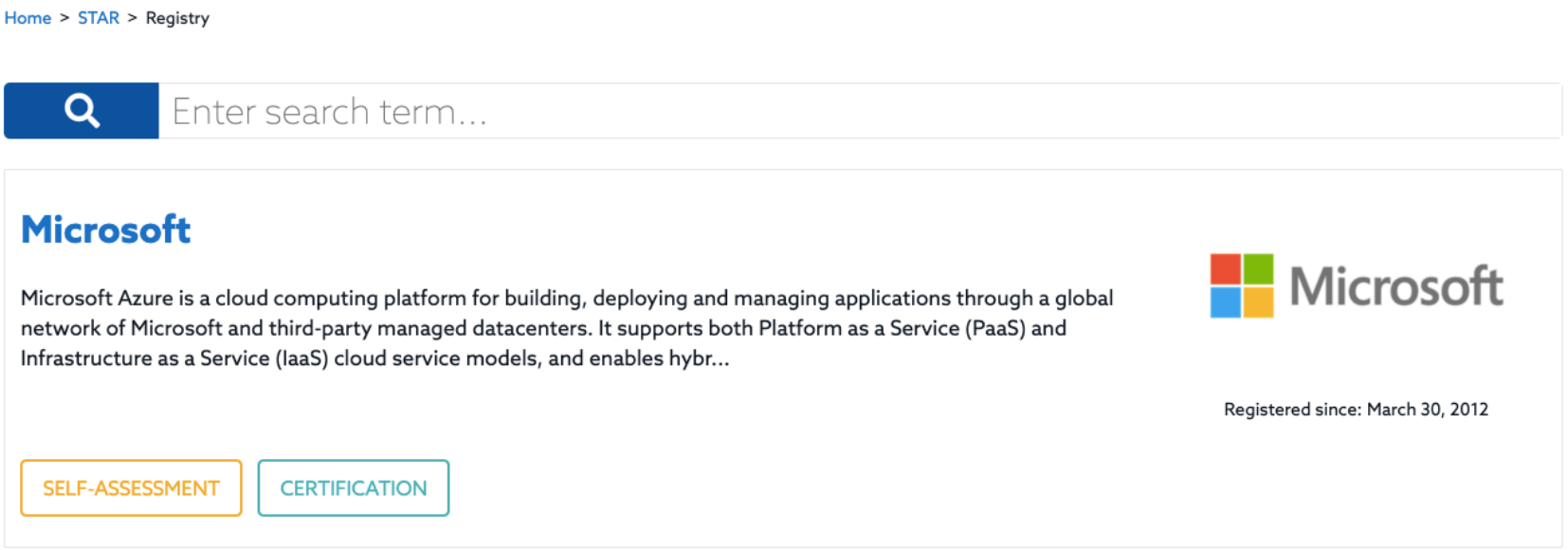
CCM

1. Application & Interface Security (AIS)
2. Audit Assurance & Compliance (AAC)
3. Business Continuity Management & Operational Resilience (BCR)
4. Change Control & Configuration Management (CCC)
5. Data Security & Information Lifecycle Management (DSI)
6. Datacenter Security (DCS)
7. Encryption & Key Management (EKM)
8. Governance & Risk Management (GRM)
9. Human Resources (HRS)
10. Identity & Access Management (IAM)
11. Infrastructure & Virtualization Security (IVS)
12. Interoperability & Portability (IPY)
13. Mobile Security (MOS)
14. Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
15. Supply Chain Management, Transparency, and Accountability (STA)
16. Threat & Vulnerability Management

Security, Trust and Assurance Registry (STAR)

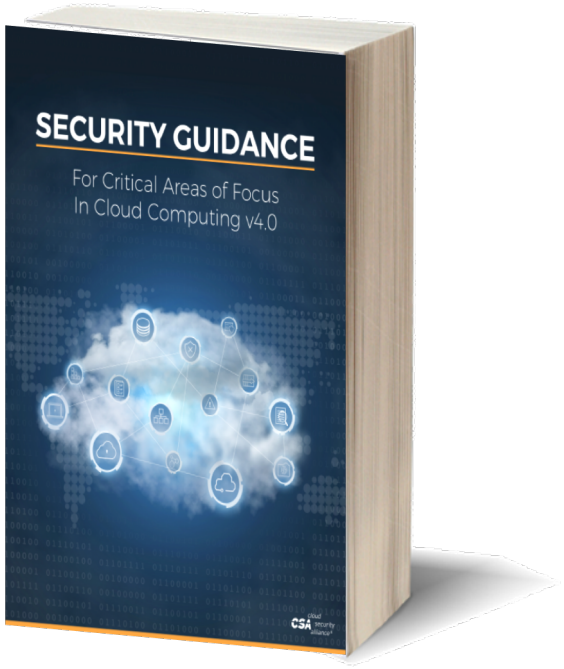
- Pour la sécurité de l'information, STAR s'appuie sur :
  - CCM
  - CAIQ
- Pour la protection de la vie privée, STAR s'appuie sur le RGPD ou GDPR

Microsoft Azure dans le registraire STAR



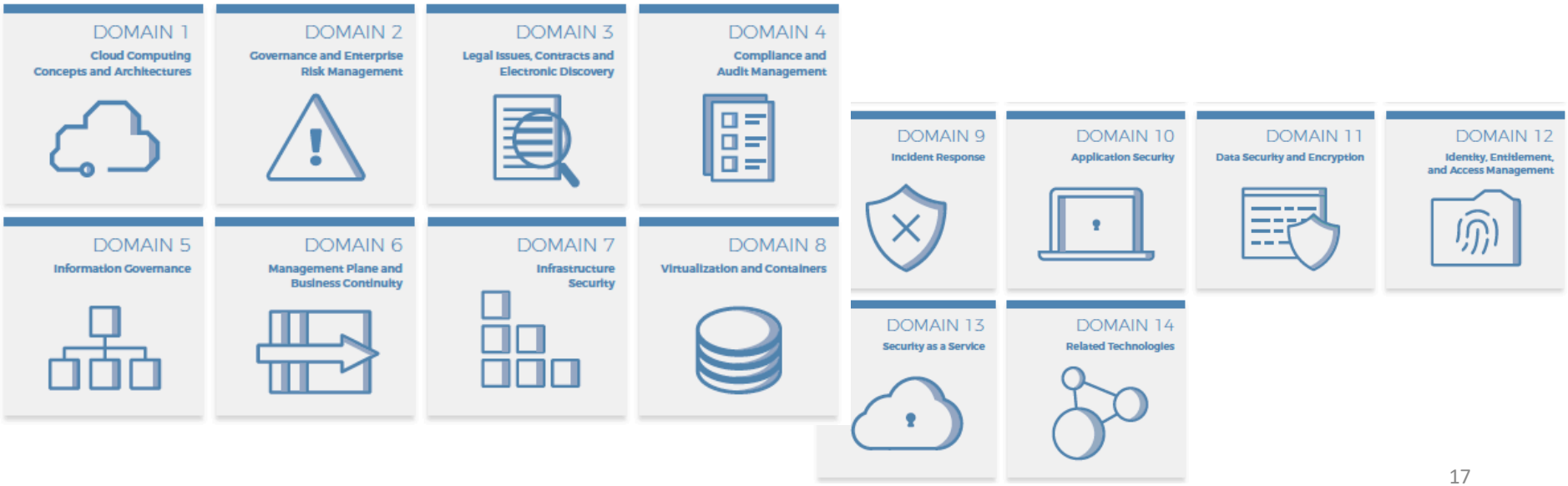
Security Guidance
For Critical Areas of Focus in Cloud Computing
v4.0

https://cloudsecurityalliance.org/download/security-guidance-v4/

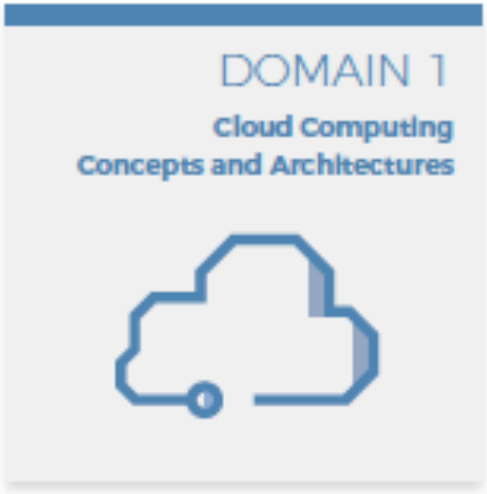


14 domaines

- Le contenu du document de la CSA se divise en 14 domaines qui couvrent l'ensemble des aspects de l'infonuagique
- Mais, il n'offre pas une grille de référence pour analyser ou évaluer les services de nature infonuagique



Domaine 1
Concepts et architectures



- Définitions
- Terminologie
- Briques fondatrices
- Éléments d'architecture : terminologie, modèles de référence

Intrants au Domaine 1 Concepts et architectures

- NIST Special Publication 800-145
  - *National Institute of Standards and Technology*
- ISO/IEC 17788:2014
  - Technologies de l'information -- Informatique en nuage -- Vue d'ensemble et vocabulaire
- ISO/IEC 17789:2014
  - Technologies de l'information -- Informatique en nuage -- Architecture de référence

Définition de l'infonuagique

- NIST
  - *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*
- ISO/IEC
  - *Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.*

- L'infonuagique est un **modèle de prestation de services TI** dématérialisée qui repose sur les technologies Internet et la virtualisation

Caractéristiques essentielles selon le NIST

1. Ressources partagées grâce à la virtualisation (*ressource pooling*)
2. Libre service et sur demande (*on-demand, self-service*)
3. Ressources sont provisionnées ou dé provisionnées (*rapid elasticity*)
4. Accessible par un réseau de type TCP/IP (*broad network access*)
5. Utilisation mesurée et éventuellement facturée (*measured service*)

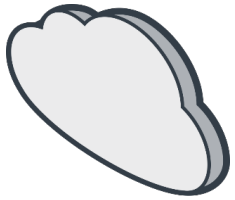
- ISO/IEC 17788 ajoute la caractéristique : *multitenancy* ou multilocataires

Qu’est-ce qui change avec le cloud ?

d’un point de vue technique

TI traditionelle

- Statique
- Manuel
- Approvisonnement par le département/service des TI
- Infrastructures dédiées



Cloud

- Dynamique
- Automatisé
- Approvisionnement en mode libre-service
- Services rendus par des fournisseurs (internes ou externes)

Les changements vont au delà de l’aspect technique

Différence entre l'infonuagique et l'impartition

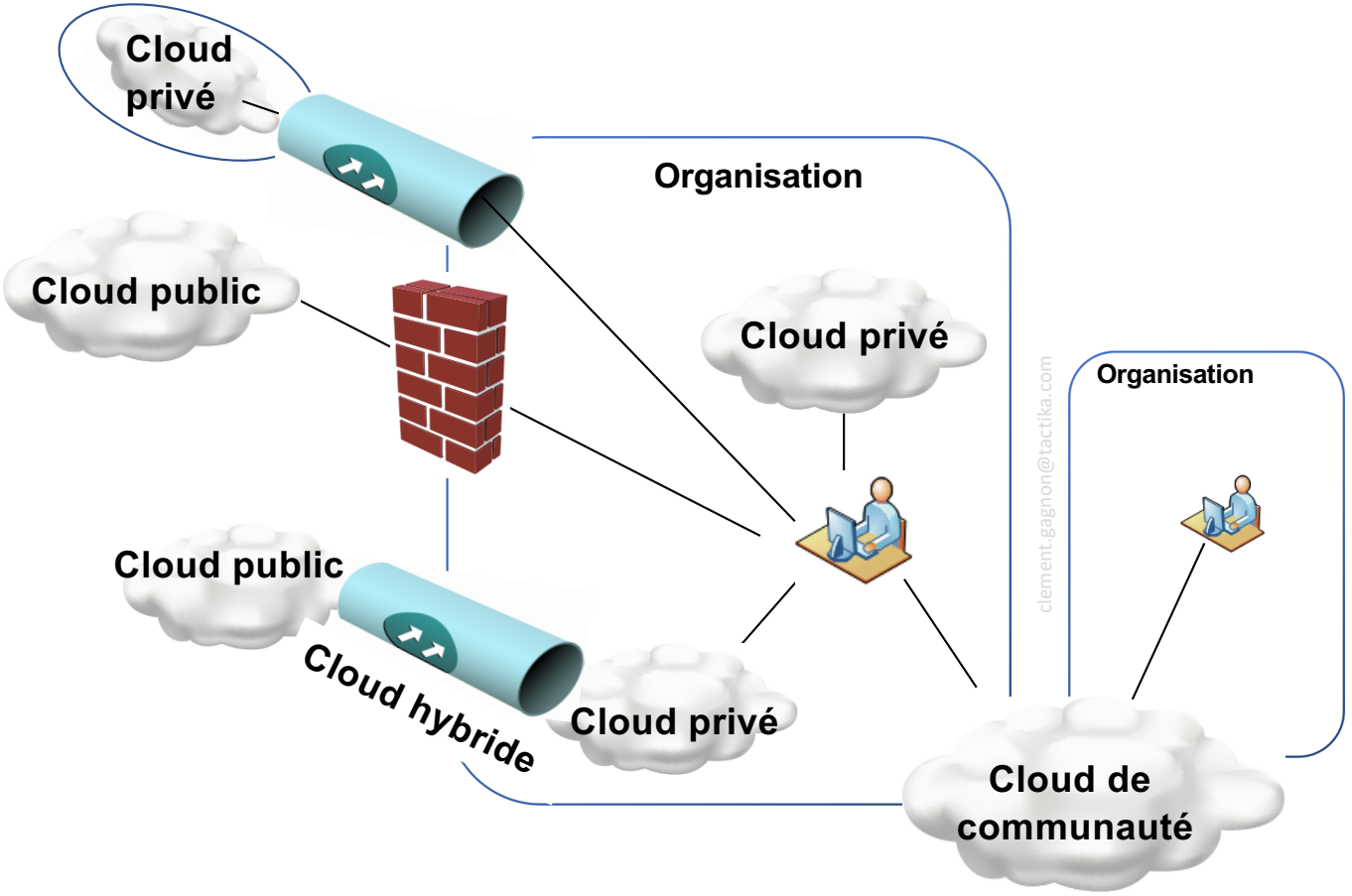
Client

Impartition
L'infrastructure est la propriété du client, non partagée,
une entente de service un à un / SLA spécifique

Infonuagique public
Infrastructure partagée, multilocataires
Même entente de service /SLA pour tous

Fournisseur

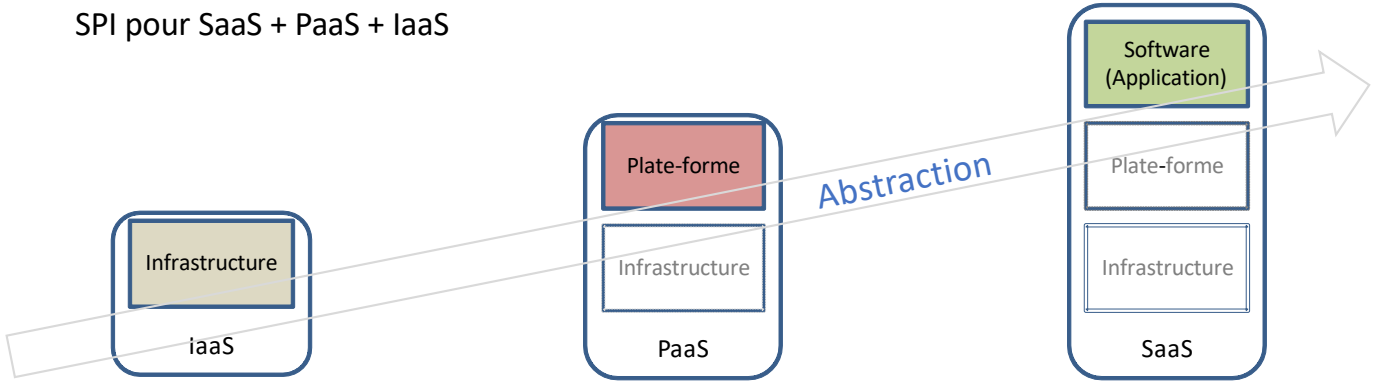
Les modèles de déploiement



Modèles de prestation de services ou modèle de service

IaaS **Infrastructure as a Service**	**PaaS** **Platform as a Service**	**SaaS** **Software as a Service** **Service as a Service**
Service de traitement (CPU), de stockage ou réseautique *Ex. Système d'exploitation Windows Server 200X, Espace disque*	Service de plates-formes applicatives avec des fonctions programmables, paramétrables, configurables *Ex. Sharepoint*	Service d'applications, Services horizontaux tel que la facturation , surveillance, sécurité, etc. *Ex. CRM (software), antivirus (service)*

SPI pour SaaS + PaaS + IaaS



Terminologie : notions d'utilisateur, fournisseur et acteur

- Utilisateur / client / consommateur
- Fournisseur / service
- Acteur / rôle (opérateur, broker, auditeur, fournisseur)

  - *Definition: A cloud user is the person or organization requesting and using the resources, and the cloud provider is the person or organization who delivers it. We also sometimes use the terms client and consumer to refer to the cloud user, and service or simply cloud to describe the provider. NIST 500-292 uses the term "cloud actor" and adds roles for cloud brokers, carriers, and auditors. ISO/IEC 17788 uses the terms cloud service customer, cloud service partner, and cloud service provider.*

Terminologie : *Management plane, Control & Data plane* et API

- *Management plane /* Couche de gestion, interface de gestion
  - Ensemble des mécanismes et dispositifs pour gérer les infrastructures
  - Metastructure
- *Control Plane*
  - *En virtualisation de la réseautique: acheminement des données et contrôle du routage*
- *Data plane* / Couche des données
  - Information : image de VM, données, etc
- *Application Programming Interface* / API
  - Une interface de programmation est une façade clairement délimitée par laquelle un logiciel offre des services à d'autres logiciels. L'objectif est de fournir une porte d'accès à une fonctionnalité en cachant les détails de la mise en œuvre (wikipedia)
  - Une **API** compatible **REST /** *Representational State Transfer*, ou « **RESTful** », est une interface de programmation d'application qui fait appel à des requêtes HTTP pour obtenir (GET), placer (PUT), publier (POST) et supprimer (DELETE) des instructions ou des données

Terminologie : Orchestration & automatisation

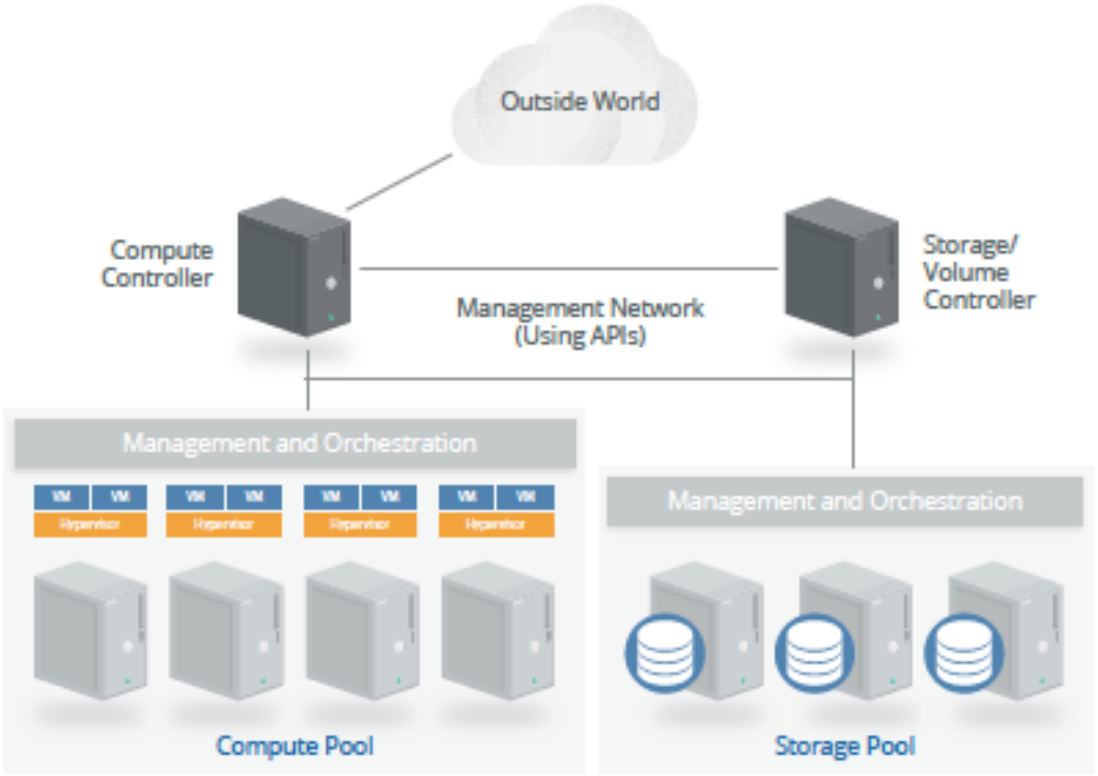
- L’orchestration est la programmation ou code qui gère les interconnexions et les interactions entre des services dans le cloud et dans le site client afin d’atteindre un résultat souhaité
- Elle transforme les tâches en flux de travail afin de pouvoir automatiser l'approvisionnement et la gestion de divers composants et leurs ressources

Terminologie: *Service Level Agreement* / SLA
Accord de niveau de service

- Entente de niveau de service
- Gestion contractuelle
- Gestion des opérations
- Qui est responsable de quoi
- Qu'elle est la législation qui est applicable lorsque désaccord ?
  - Préséance
  - Etc …

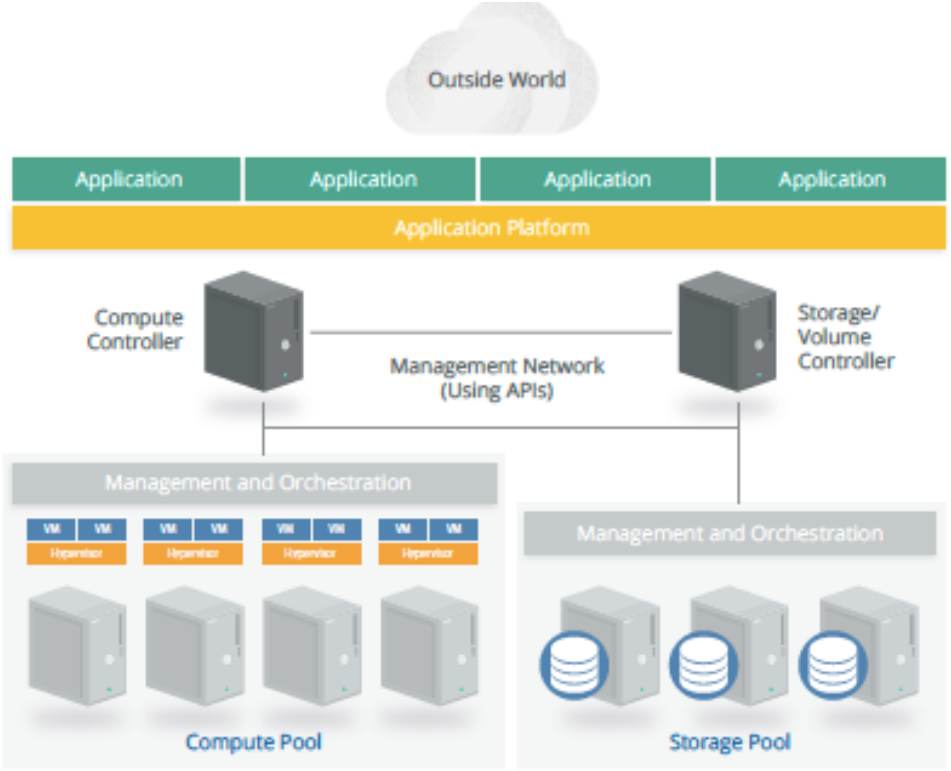
Infrastructure as a Service / IaaS

- Représentation simplifiée d'une infrastructure IaaS
- Éléments importants
  - Contrôleurs
  - Management & orchestration
  - API
  - Virtualisation et hyperviseurs



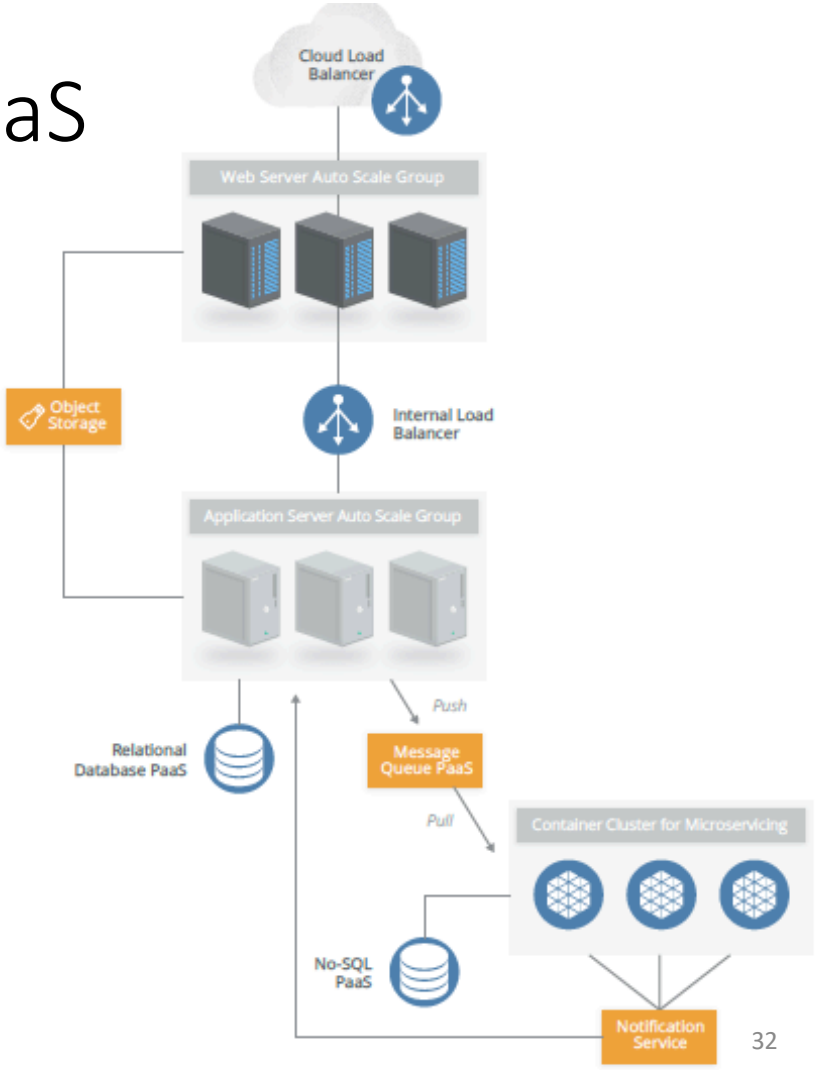
Platform as a Service / PaaS

- Représentation simplifiée d'une infrastructure PaaS
- Définition parfois floue
- Essentiellement, c'est une couche au dessus de IaaS
- Ex: DBaaS, environnement de dev
- Élément important : API



Software as a Service / SaaS

- Représentation simplifiée d'une infrastructure SaaS
- Elle peut combiner plusieurs services provenant de fournisseurs différents
- Les utilisateurs peuvent utiliser plusieurs dispositifs : web, applications mobiles, API

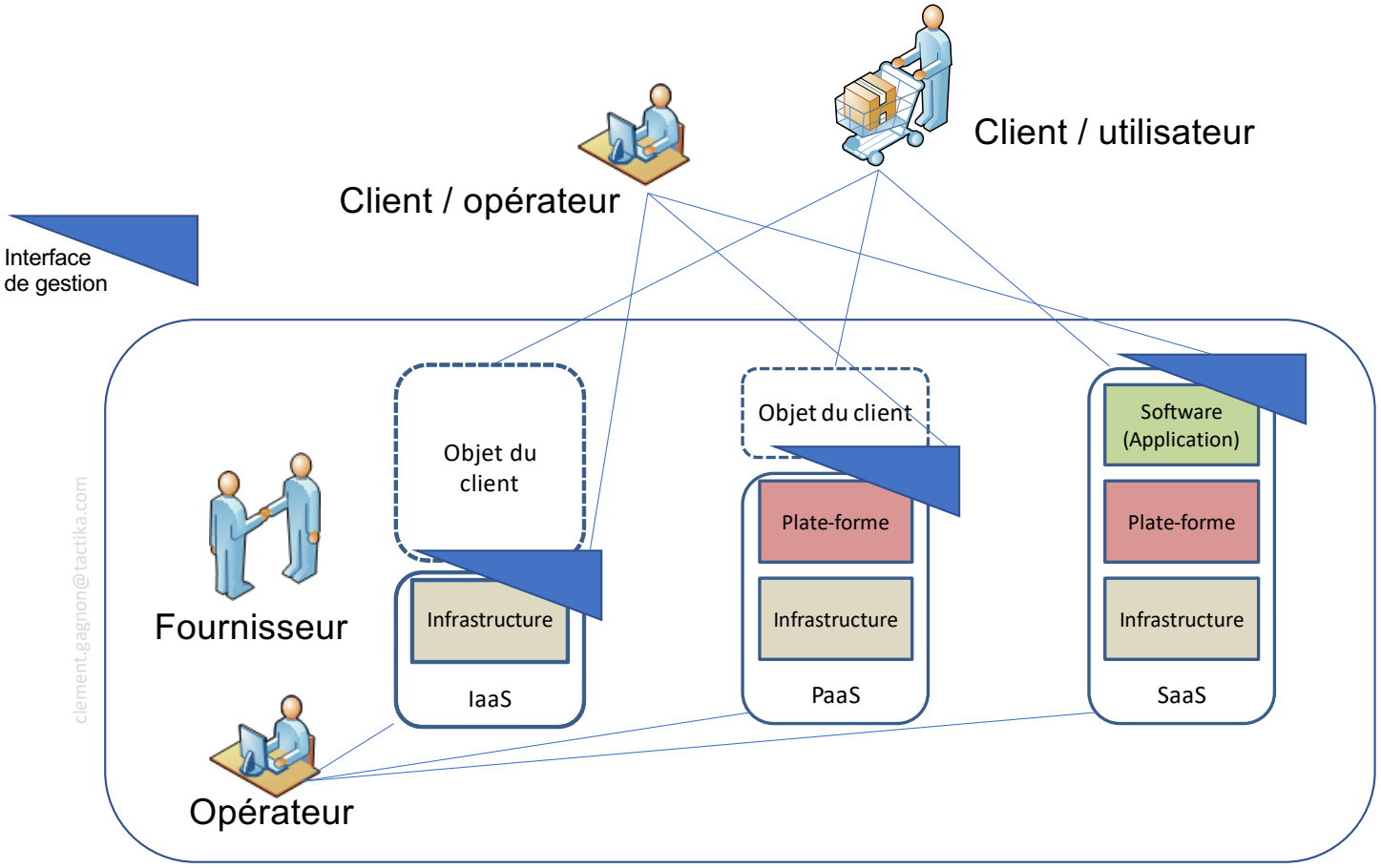


X as a Service

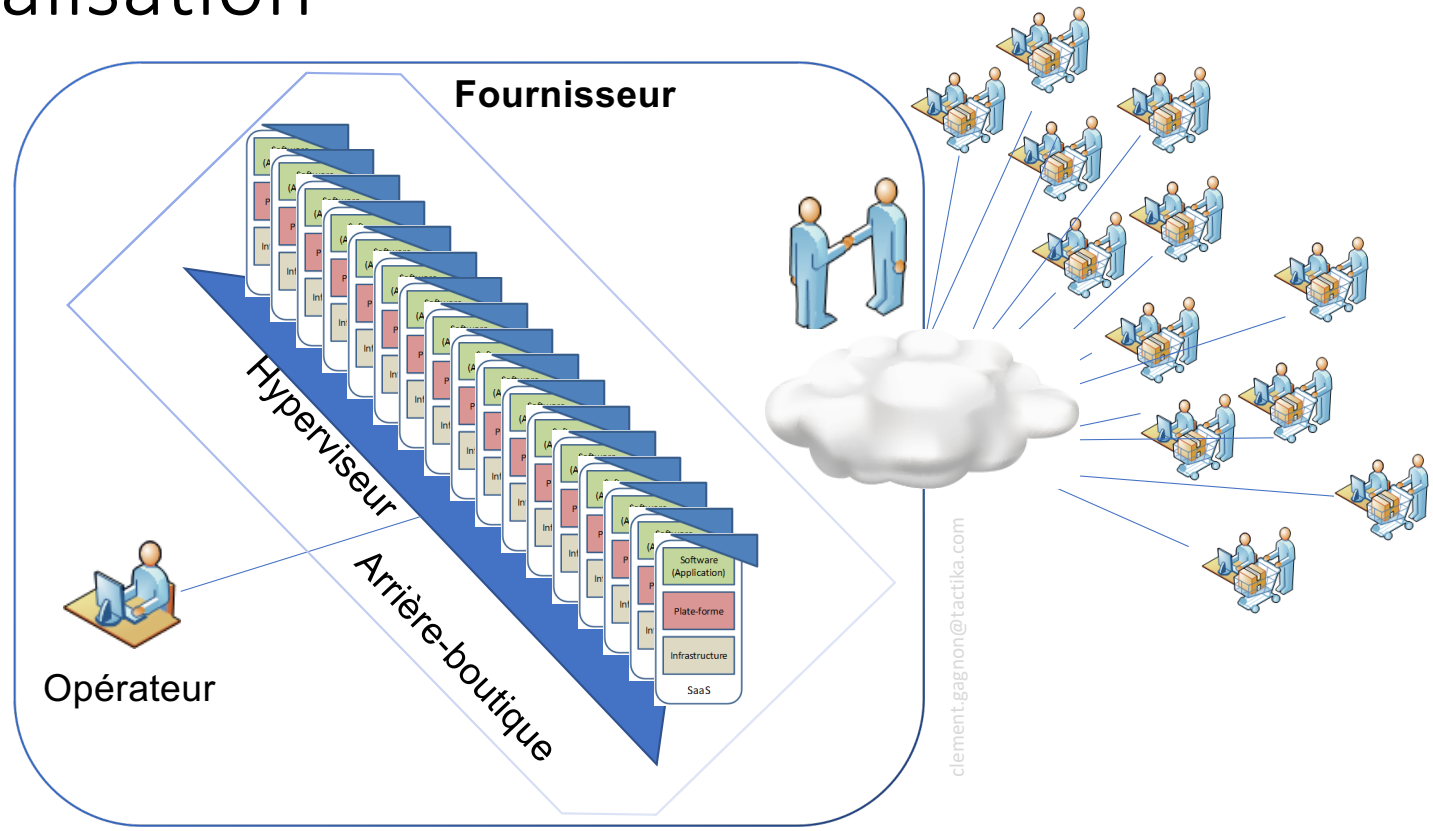
Catégories de services cloud	Infrastructure	Platform	Application
Software as a Service			X
Platform as a Service		X	
Infrastructure as a Service	X		
Network as a Service	X	X	X
Data Storage as a Service	X	X	X
Compute as a Service	X		
Communication as a Service		X	X
Database as a Service		X	X
Desktop as a Service			X
Security as a Service	X	X	X

ISO/IEC DIS 17788

Les acteurs dans les modèles de services



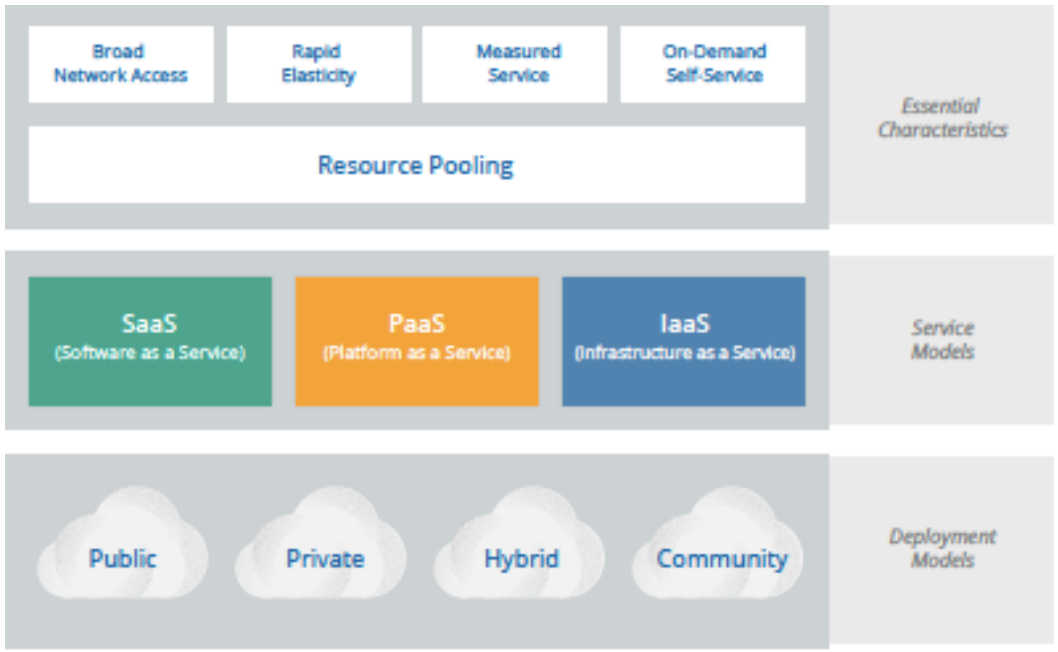
Vue fournisseur : partagé, multilocataires, virtualisation



clement.gagnon@tactika.com

Vue synthétique des modèles

- Caractéristiques essentielles
- Modèles de service
- Modèles de déploiement



Lien entre les acteurs

Cloud privé intramuros

Cloud privé chez un fournisseur

	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization	Organization	On-Premises	Trusted
	Third-Party Provider	Third-Party Provider	Off-Premises	
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

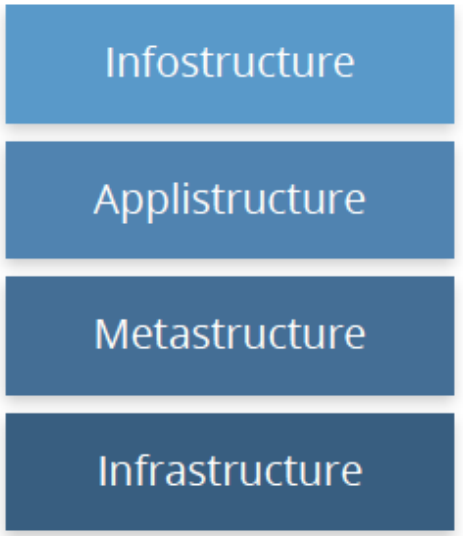
Lien entre les acteurs

Cloud privé fourni et géré par un fournisseur intra muros

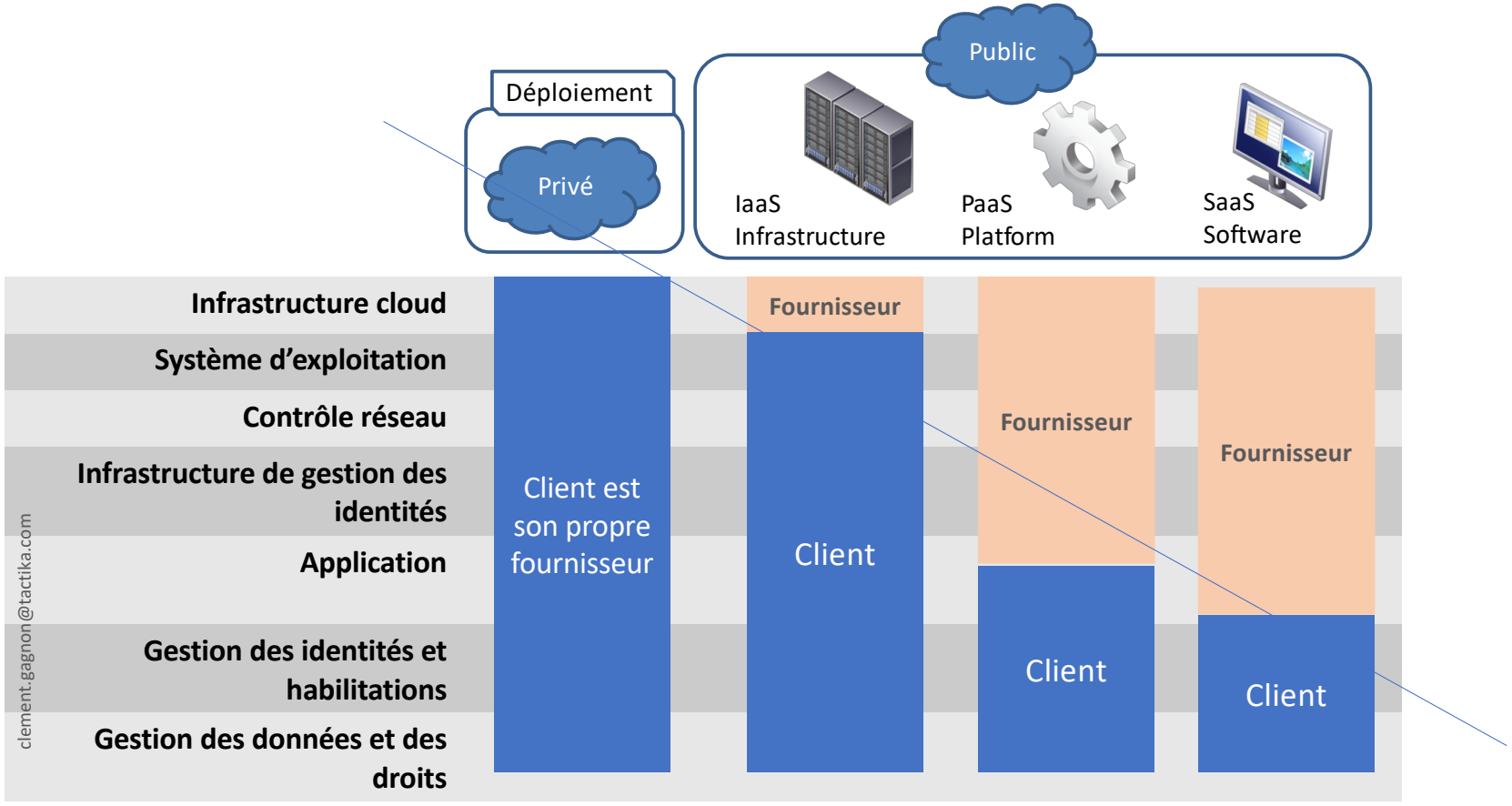
	Infrastructure Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third-Party Provider	Third-Party Provider	Off-Premises	Untrusted
Private/ Community	Organization Third-Party Provider	Organization Third-Party Provider	On-Premises Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

Modèle logique

- **Infostructure**
  - Données et autres informations, ex: Base de données
- **Applistructure**
  - Applications déployées dans le nuage et l'arrière boutique
    - Ex: PaaS peut requérir les services de messages queueing, notifications, IA, etc
- ***Metastructure***
  - Mécanismes et protocoles qui interfacent l'infrastructure avec les autres couches pour la gestion et la paramétrisation
- **Infrastructure**
  - Éléments physiques : *compute, network, storage*
- La principale différence entre le cloud et l'infrastructure traditionnelle se situe à la Metastructure : Management plane
- Les besoins de sécurité, les processus et les technologies se distinguent selon la couche



Partage <u>générique</u> des responsabilités



* Cas génériques

Mots clés et concepts à assimiler et à maitriser

- Virtualisation
- Abstraction
- *Application Programming Interface* / API
- Orchestration & automatisation
- *Cloud management plane*
- Gestion contractuelle & accord de niveau de service/ *Service Level Agreement* / SLA
- Partage des responsabilités

Domaine 2: Gouvernance et gestion des risques de l'entreprise

- Définition du risque
- Gestion des risques
- Gouvernance et infonuagique

La perception du risque et le Cloud

En affaires, le risque est perçu comme une opportunité ou comme un événement négatif.

Les bénéfices du Cloud sont une opportunité. Une organisation peut démontrer un appétit et une tolérance aux risques dans sa recherche d'opportunités.

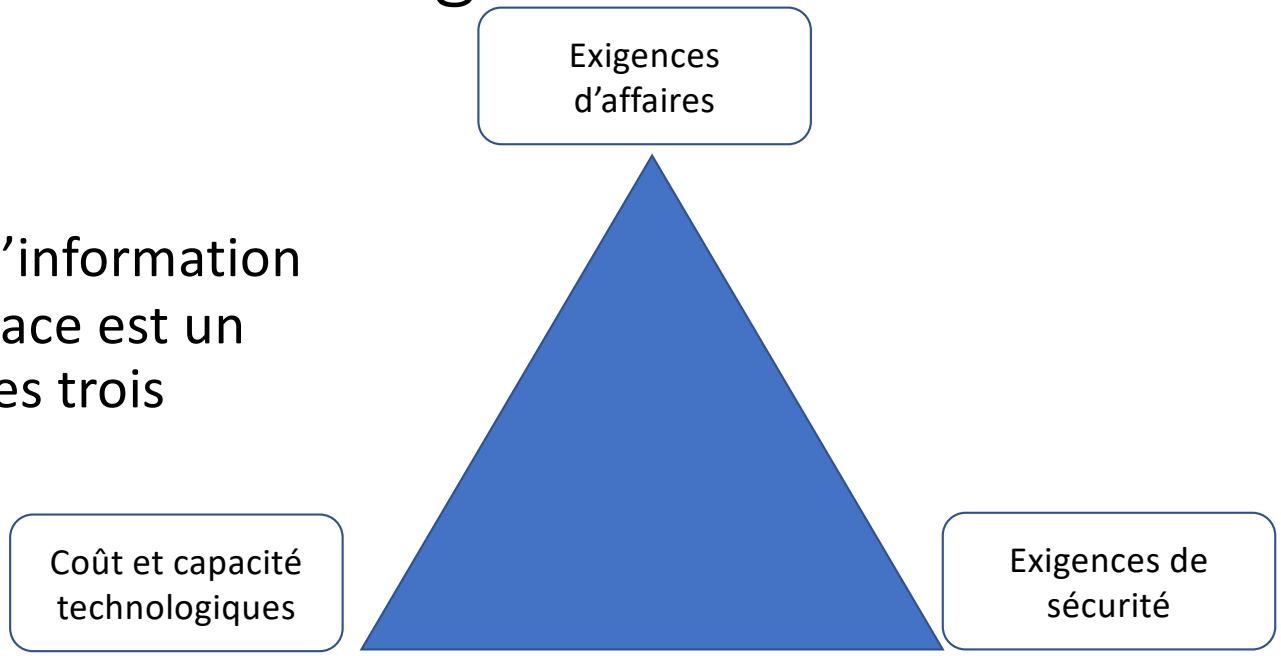
En sécurité de l'information, le risque est perçu comme une menace qui met en péril l'atteinte des objectifs.

Les problèmes du Cloud :

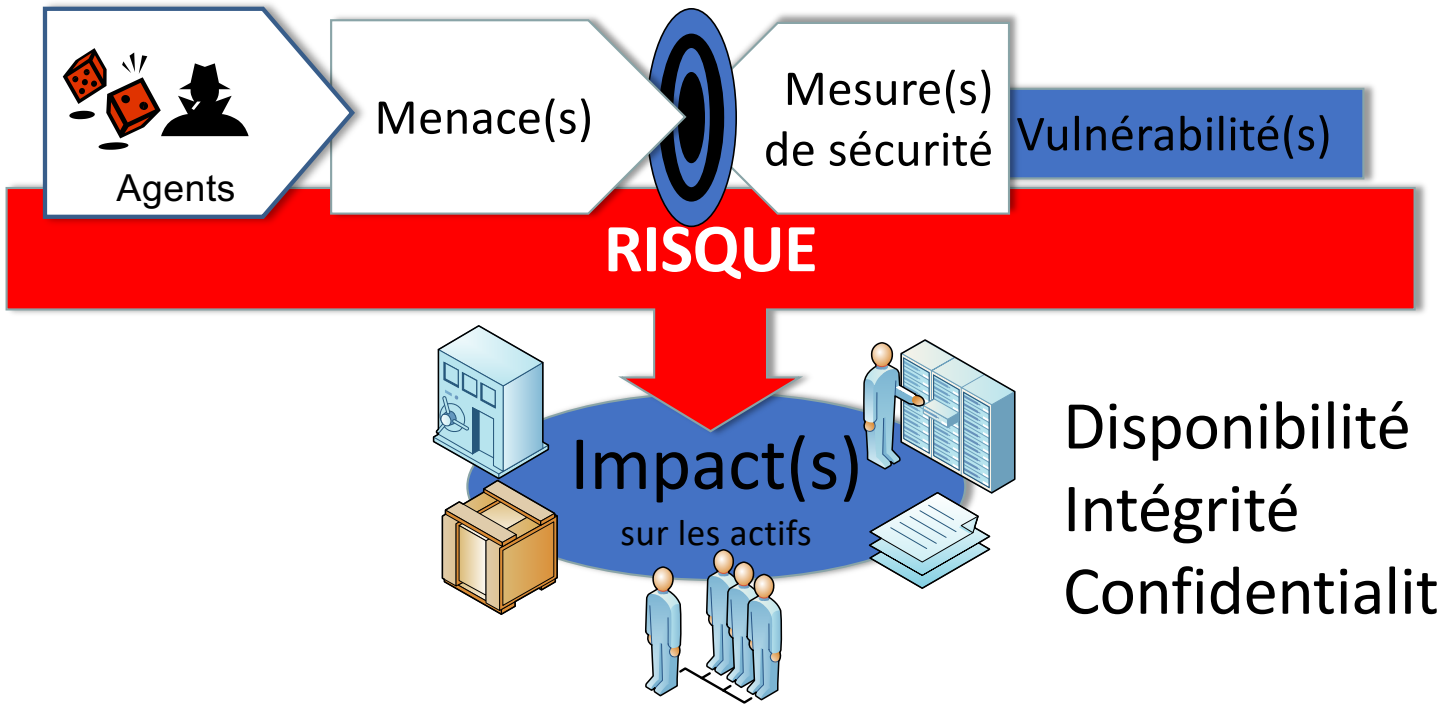
- Les risques d'un tiers peuvent devenir mes risques ...
- Si plusieurs tiers sont impliqués, les risques des tiers sont «chainés».

Équilibre entre la sécurité, les exigences d'affaires et la technologie

- Une sécurité de l'information efficiente et efficace est un équilibre entre ces trois éléments



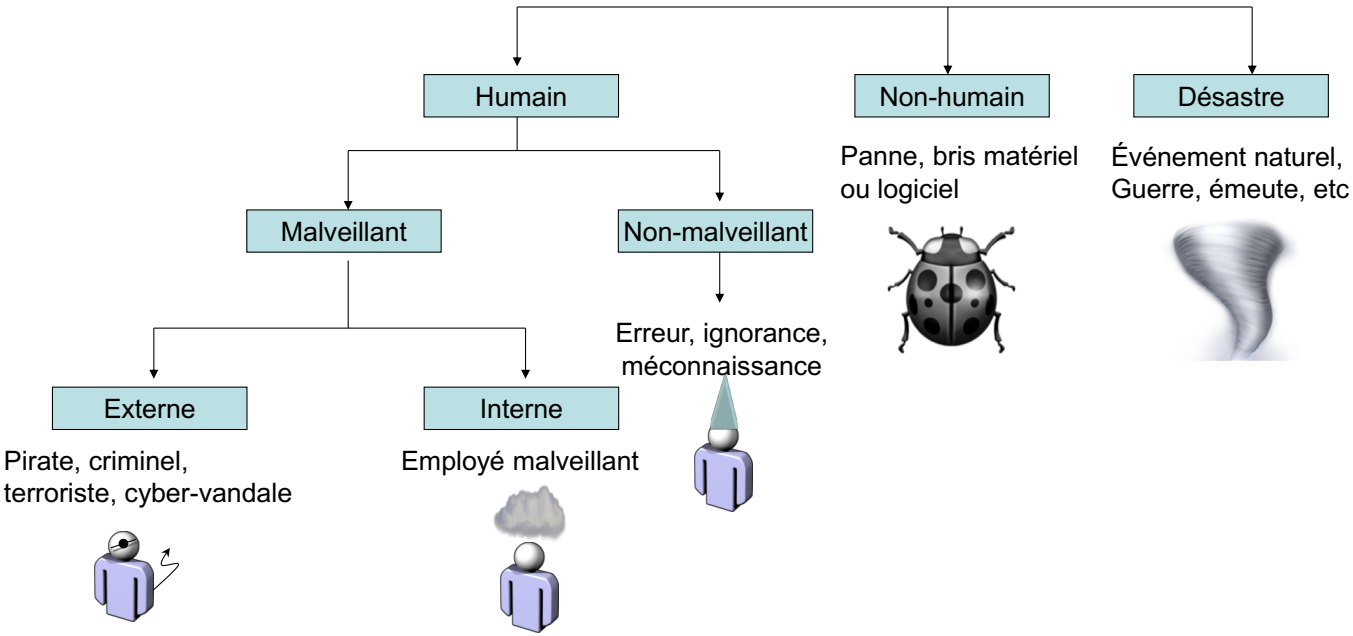
La mécanique du risque



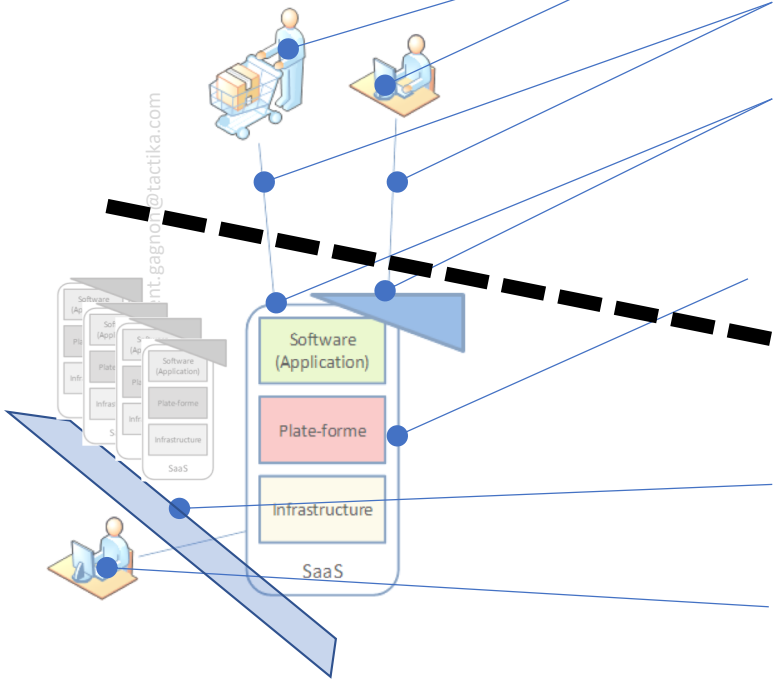
Disponibilité
Intégrité
Confidentialité

Agents & probabilité

Probabilité : Événement extérieur, imprévisible, irrésistible et insurmontable de nature à dégager de toute responsabilité, usure, fin de vie de matériel



Aperçu des menaces pour le cloud



Humain : ingénierie sociale, malveillance
Client Web : Code malveillant, XSS (*cross site scripting*), *Phishing,* DNS *poisoning*

Panne, désastre, Interception (MITM), déni de service

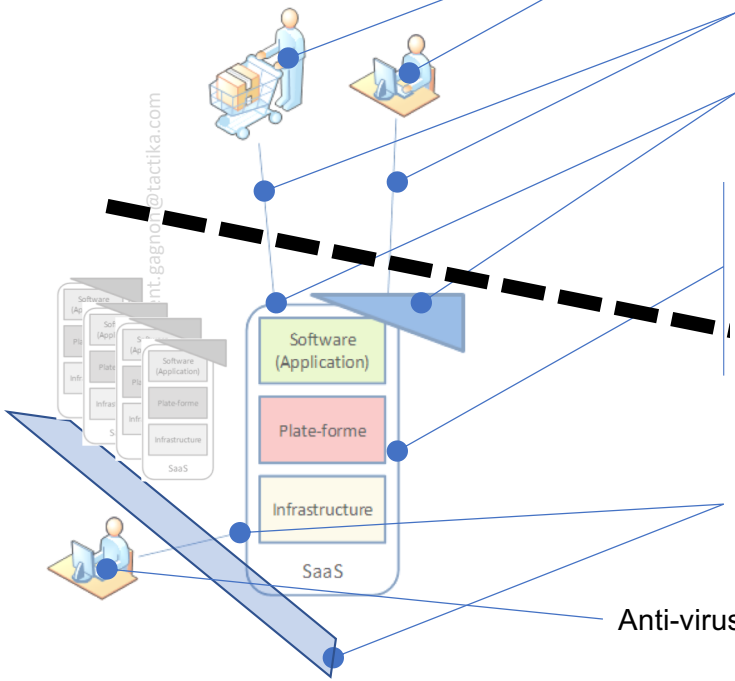
BOF, Injection SQL, Déni de service, Attaque brute sur l'authentification

Changement non annoncé ou non planifié
Code malveillant, Attaque brute sur l'authentification, Attaque sur l'hyperviseur, Déni de service

Panne, désastre,
injection de code, mauvaise paramétrisation

Humain : ingénierie sociale, malveillance
Client Web : Code malveillant,
XSS (*cross site scripting*), *Phishing,* DNS *poisoning*

Principales mesures de contrôle



Anti-virus, anti-logiciel espion, correctif

Chiffrement, lien sécurisé
Relève, redondance

Contrôle d'accès authentification (forte), réseau
Détection des intrusions

Contrôle d'accès physique de l'infrastructure
Contrôle d'accès authentification (forte), réseau
Signature et chiffrement
Contrôle des vulnérabilités : correctifs
Relève, redondance
Journalisation, anti-virus, anti logiciel-espion, IDS/IPS

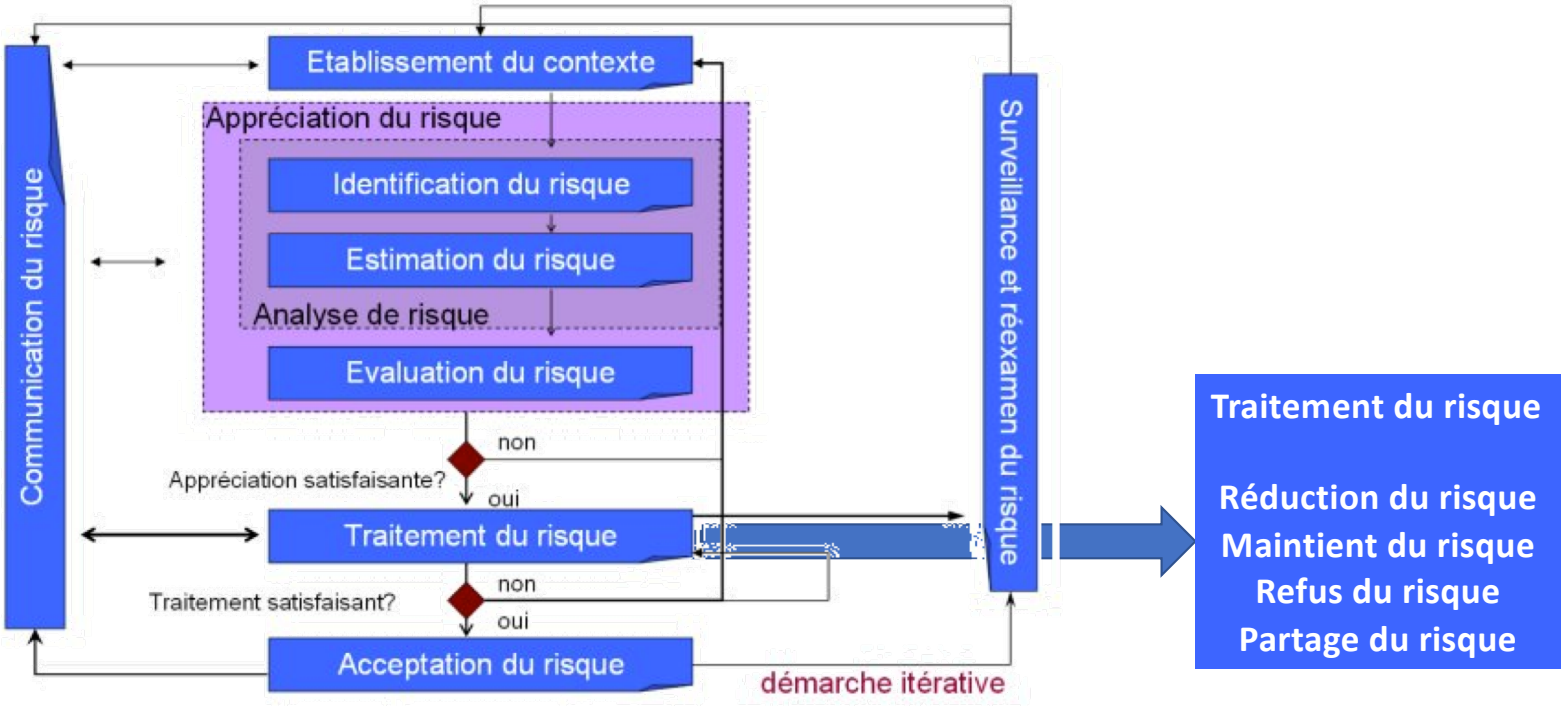
Contrôle d'accès : authentification (forte) & réseau
Détection des intrusions, journalisation

Anti-virus, anti-logiciel espion, correctif

Démarche de gestion du risque ISO27005

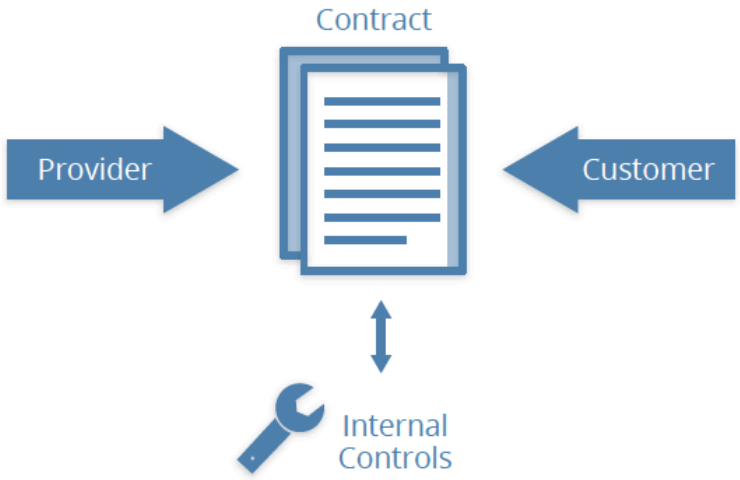
ISO/CEI 27005:2008

Gestion des risques en sécurité des systèmes d'information



Outils de la gouvernance pour l'infonuagique

- **Contrats**
- **Évaluations (assessment) du fournisseur**
  - Sécurité, performance, processus
- **Rapports de conformité**



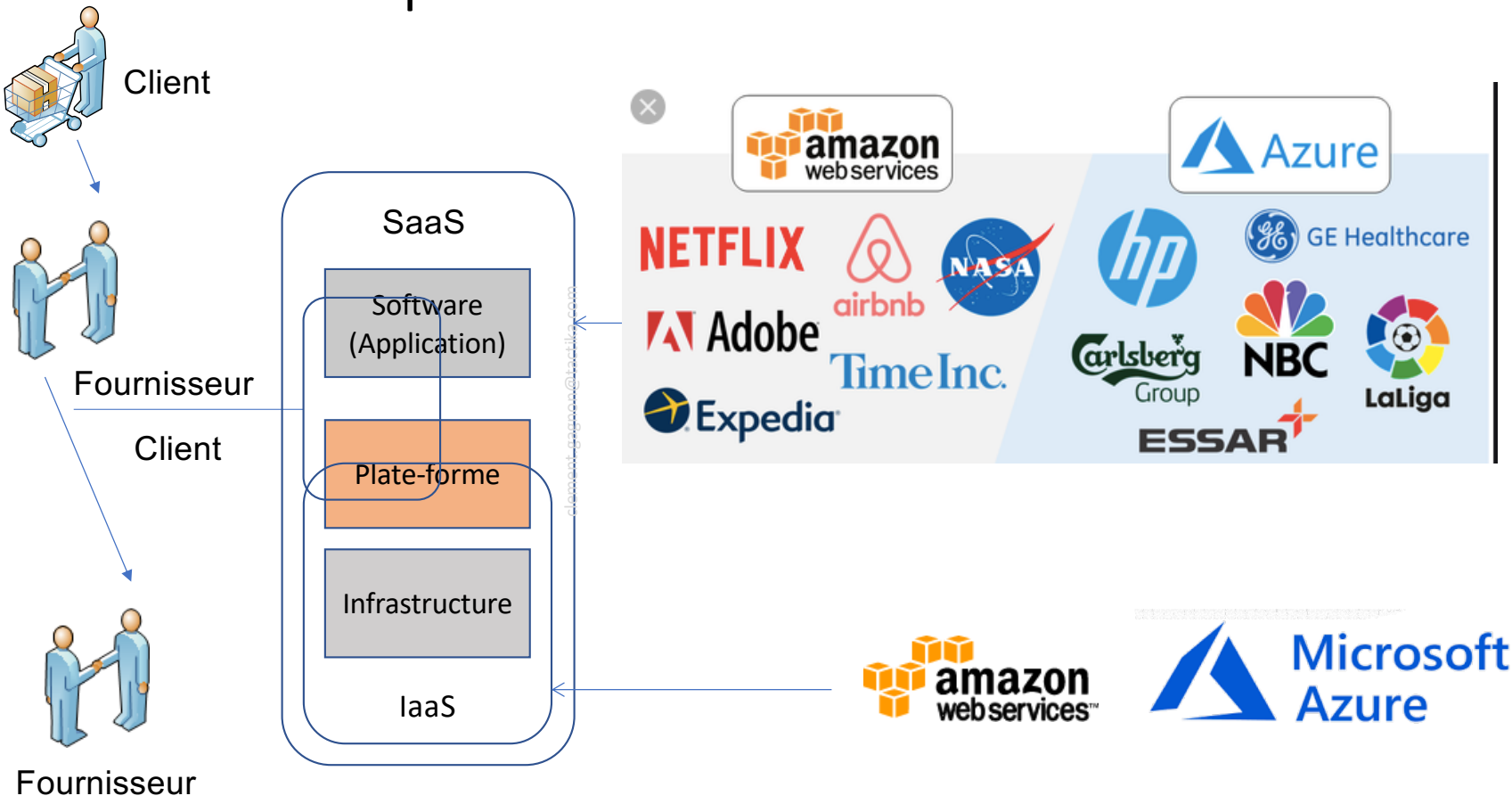
- *Cloud Security Alliance STAR Registry*
  - Programme de certification, d'assurance et registre de documentation basé sur CSA CCMC

Entreprise Risk Management / ERM

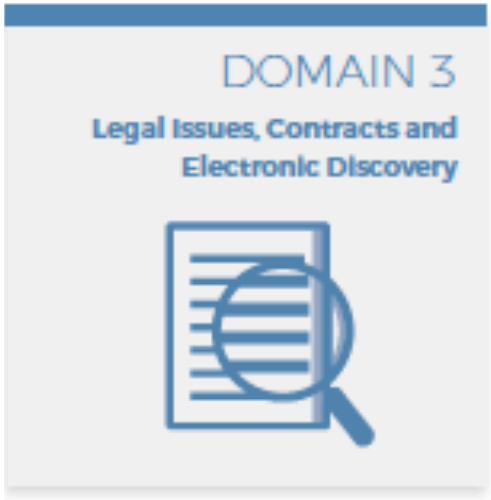
- Gestion des risques dans une organisation
- Appétit et tolérance aux risques
- Infonuagique
  - Le risque est partagée
    - Client/consommateur et le fournisseur

- Référence
  - *ISO/IEC 31000:2009 Risk Management – Principles and guidelines*
  - *ISO/IEC 31010:2009 Risk Management – Risk assessment techniques*
  - *Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach, NIST Special Publication 800-37 Revision 1*

Chaîne des risques et des tiers



Domaine 3: Considérations légales, contractuelles et forensiques/analyse judiciaire



- Obligations légales
- Contrats et SLA
- Déclarations des brèches de sécurité
- Collecte de preuves
- Protection de la vie privée
- Juridiction des pays impliqués
- Interactions avec des tiers

Thèmes communs

- La plupart des législations possède ces thèmes communs
  - Protection de la vie privée
  - Mesures de sécurité de base
  - Restrictions sur le transit des données entre des états

Cadre légal de la protection des données et de la vie privée

- Parfois, l'implication de plusieurs législations nationales selon le lieu de la collecte, du traitement et de la consommation
  - **Localisation**
    - Du fournisseur de service
    - De l'utilisateur
    - De la nature des données
    - De la localisation des serveurs
  - **Juridiction**
    - Sous laquelle le contrat est rédigé pour les parties impliquées

Résumé des principales législations

- Dans le guide :
  - Asie et région du Pacifique
    - Australie, Chine, Japon et Russie
  - Amérique
    - Amérique centrale et Amérique du Sud
    - Etats-Unis
    - Canada ??? → pas de mention dans le document
  - Europe et l'Union Européenne (voir GDPR)

Règlement général sur la protection des données / RGPD
General Data Protection Regulation / GDPR

- Le Règlement général sur la protection des données (RGPD) (*General Data Protection Regulation*, *GDPR*) constitue le nouveau texte de référence européen en matière de protection des données à caractère personnel
- ll renforce et unifie la protection des données pour les individus au sein de l'Union européenne
- S'applique aux organisations qui traitent/manipulent/entreposent les informations personnelles des européens, elles sont soumissent à la supervision des autorités les plus proches
- Effectif depuis mai 2018

Pratiques recommandées

- Avoir un processus de gestion contractuelle adaptée à l'infonuagique
- Vérifier les lois, les règlements et les pratiques recommandées applicables dans le projet infonuagique
- Établir des processus et des mécanismes de surveillance, d'évaluation et de mise à jour
- Établir des processus et mécanismes d'évaluation et de vérification par un tiers
  - Audits et attestations

Un conseil …

- Selon l'envergure du service, la valeur et la sensibilité des données
  - Il est préférable de demander un avis légal au moment opportun
    - À une ressource légale qui a des connaissances techniques minimales …

- Il est mieux d'investir quelques $ avant que de perdre plusieurs $$$ après …

Informatique légale / *Electronic discovery*

- Réponse à un subpœna ou citation à comparaitre
- Demandeur qui veut obtenir des documents dans le cadre d'un litige
- Propriété, possession, contrôle, préservation, gestion de la preuve
- Implication d'un fournisseur (application et environnement cloud) lors d'un litige entre un demandeur et un défendeur
- Outils de recherche et forensique dans un grand volume de données
- Durée de conservation et de préservation des informations selon la réglementation
- Collecte d'informations
- Accès à l'information
- Format des données
- Authentification
- Coopération entre les parties dans la recherche légale

Domaine 4: Conformité et audit

- Impact de l'infonuagique pour les données et applications dans le nuage
- Conformité avec les politiques de sécurité, les lois et règlements

Terminologie: conformité et audit

- Conformité
  - La **conformité** est l'état de ce qui présente un accord *complet*, une adaptation *totale*. … on utilise fréquemment le terme anglais ***compliance***. (wikipédia)
  - satisfaction d'une *exigence* (ISO/IEC 27000:2018(F))
- Audit
  - *processus* méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits (ISO/IEC 27000:2018(F))

Cloud et conformité

- La conformité, comme la sécurité, est partagée entre le client et le fournisseur
- Le client est toujours l'ultime responsable de SA conformité
- Les responsabilités sont définies par les contrats, les lois et règlements applicables
- Les audits et vérifications permettent de confirmer la conformité du fournisseur et/ou celle du client
- L'exercice peut être réaliser par un « interne » de l'organisation du client ou du fournisseur ou par un tiers
- Il est possible que des lois ou règlements impose un *modus operandi* à l'audit ou la vérification de la conformité

Législations et les pratiques de l'industrie

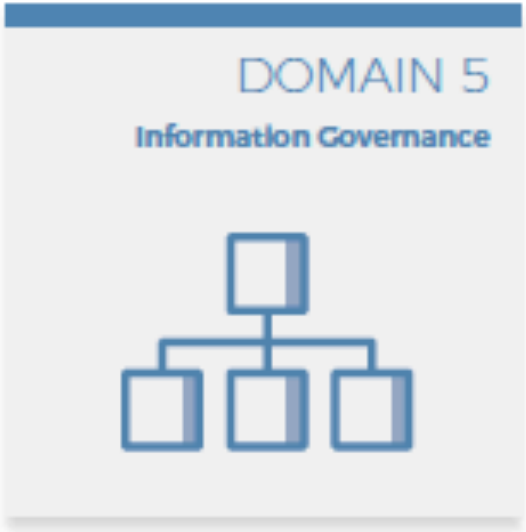
- Le CSA *Cloud control Matrix* (CCM) permet faire des liens et assurer une cohérence entre les normes et lois
  - *Payment Card Industry Data Security Standard* / PCI DSS
  - *Audit Service Organization Control (SOC)* / SOC1 et SOC2
    - *The American Institute of Certified Public Accountants* (AICPA)

      https://www.ispartnersllc.com/blog/soc-1-soc-2-reports-difference/
  - *Statement on Standards for Attestation Engagements No. 16 /* SSAE 16
    - Remplacé par SSAE 18 en mai 2017
    - Publié par *Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants / AICPA*
    - A remplacé le *Auditing Standards No. 70* / SAS 70
  - *Health Insurance Portability and Accountability Act /* HIPAA
    - Loi votée par le Congrès des États-Unis en 1996 et qui concerne la santé et l'assurance maladie
  - Règlement général sur la protection des données / RGPD
    General Data Protection Regulation / GDPR

Enjeux des régulations et le cloud

- Délimiter la portée de la législation
- Les mesures de contrôle sont parfois sujettes à interprétation
- Les fournisseurs doivent documenter comment ils réalisent la conformité
- Être en état de conformité ne veut pas dire être « totalement » sécuritaire

Domaine 5: Gouvernance informationnelle



- Besoin d’affaires et conformité
- Cycle de vie des données

Définition

- Gouvernance informationnelle
  - S'assurer que l'exploitation des données est conforme avec la stratégie, les politiques, les normes, les lois et les règlements, les ententes contractuelles et les objectifs d'affaires de l'organisation

Ensuring the use of data and information complies with organizational policies, standards and strategy — including regulatory, contractual, and business objectives.

Différence entre information et donnée

- L'information est une donnée avec de la valeur
  (Définition du CSA, traduction libre)
- Cependant, les deux termes, information et données, sont utilisés d'une façon interchangeable

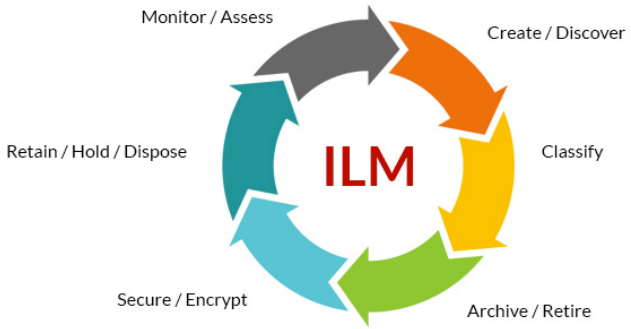
Gouvernance informationnelle et infonuagique

- Impacts de l'utilisation de l'infonuagique sur la gouvernance informationnelle
- Les éléments sont :
  - Politique de gestion de l'information / Gestion des actifs
    - Classification et catégorisation
    - Propriété, conservateur, gardien, mandataire
  - Législation et localisation
    - Juridiction applicable et souveraineté
    - Conformité, régulation et protection des données et de la vie privée
  - Obligations contractuelles
    - Responsabilité partagée de la sécurité
  - Mesures de contrôle de sécurité (pratiques recommandées, normes)
    - Habilitation (autorisation)
    - Services partagées (*multitenancy*)
    - Destruction et disposition des données

Localisation, obligation contractuelle et législation

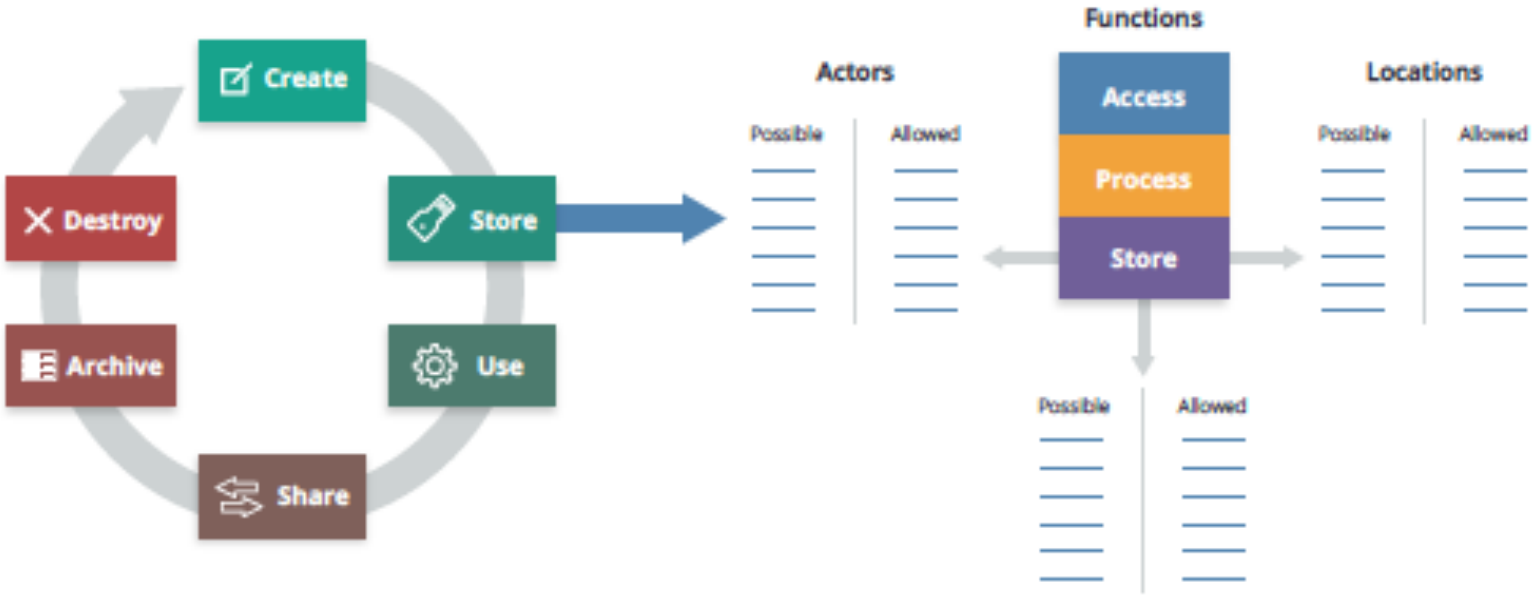
- Droits et permissions
  - Qui doit accéder les données ?
    - Quelles sont les juridictions qui doivent s'appliquer ?
  - Comment ces données sont accédées ?
    - Selon les mécanismes d'accès, quels sont leurs capacités de protection ?
  - Comment sont-elles détruites ?
  - Etc.

Cycle de vie des données

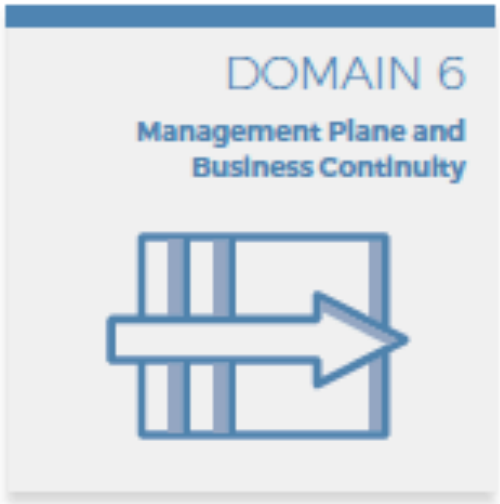


Cycle de vie de l'information (ILM)

Mapping du cycle de vie et des accès et manipulation



Domaine 6: Gestion de l’infrastructure et continuité des affaires



- Protection du service de gestion de l’infrastructure
- Des consoles, des interfaces API
- Assurer la continuité des services

Management plane / Interface de gestion

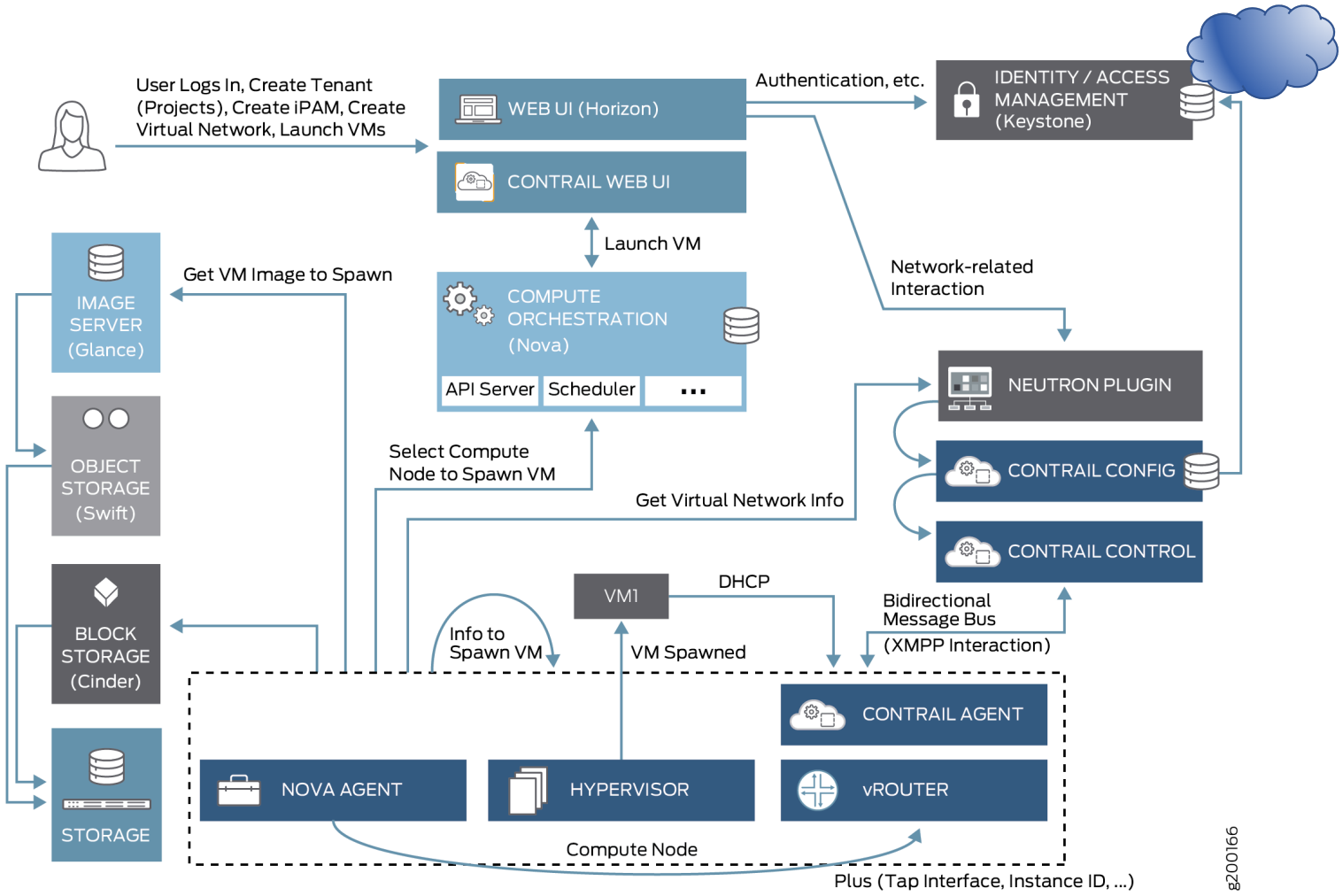
- Élément majeur, ce sont les « joyaux de la couronne »
- Interface vers la métastructure et la configuration cloud
- Sous la responsabilité du fournisseur de service

Sécurité de l'interface de gestion

- Éléments important pour sécurité l'interface
  - Contrôle d'accès à l'API
  - Sécurité du périmètre, contrôle réseautique
  - *Identity and Access Management* / IAM
    - Identité/ **Authentification** / Autorisation
    - Authentification du client , MFA
    - Authentification interne et propagation de celle-ci
  - Journalisation, surveillance et alertage

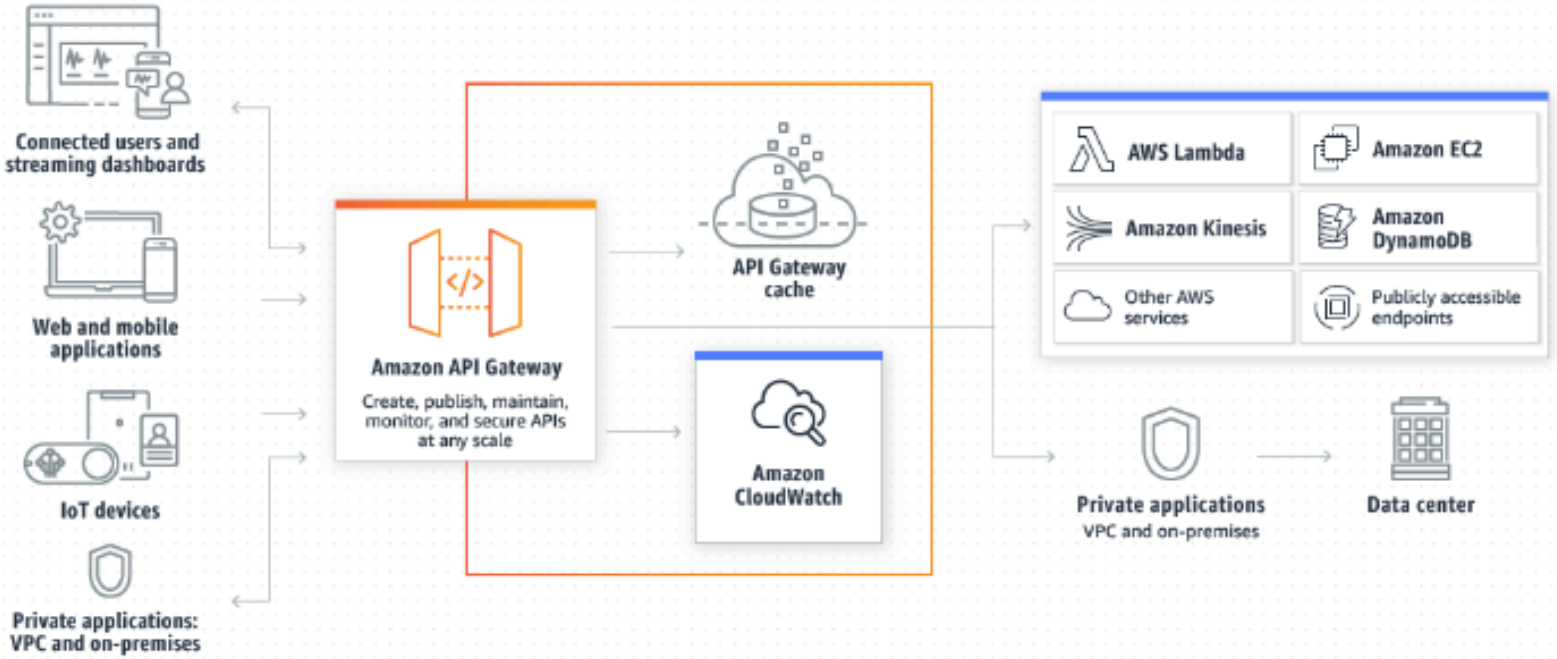
Exemple des échanges dans le Management Plane
dans une infrastructure infonuagique

- Console
- Authentification
- Autorisation
- Orchestration
- API



Extrait de la documentation Contrail Cloud Juniper

Exemple d'utilisation des API avec une passerelle vers le Management Plane dans une infrastructure infonuagique



Extrait de la document AWS, Amazon API Gateway

Continuité de service et relève

- Un plan de continuité des activités (CA)
  - Plan visant la poursuite des opérations d'une entreprise en cas de sinistre ou d'interruption.
- La reprise après catastrophe (RC)
  - Ensemble de politiques et de procédures permettant la reprise des activités des principaux systèmes de TI à la suite d'un sinistre ou d'une interruption.

- *Business Continuity & Disaster Recovery* / BC & DR

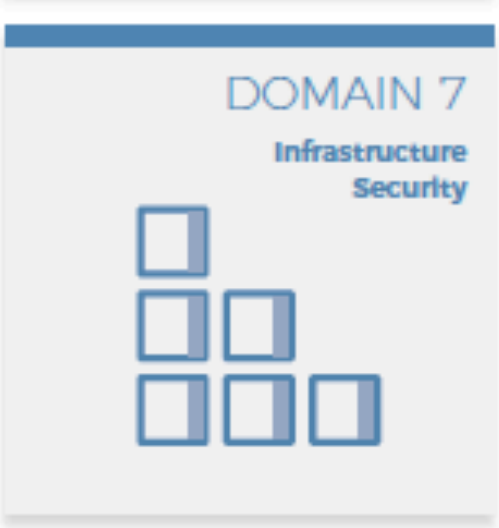
http://www.directioninformatique.com/commandite/reprise-apres-catastrophe-et-continuite-des-activites-deux-choses-differentes

Business Continuity & Disaster Recovery / BC & DR

- Le désastre peut être « *act of god* » ou de source malveillante
- Architecturer pour la défaillance
- Dans le cloud, c'est une responsabilité partagée
- Une approche par le risque est préconisée
- Le plan doit être documenté (client et fournisseur)
- Les fournisseurs cloud ne sont pas tous créés égaux !

  Perte de données maximale admissible / PDMA
  Recovery point objective / RPO
  Durée maximale d'interruption admissible / DMIA
  Recovery time objective / RTO

Domaine 7: Sécurité de l'infrastructure



- Sécurisation de l'infrastructure réseautique et de traitement
- Infrastructure réseau
- VLAN, SDN, SDP, *appliance* virtuelle

Les couches d'infrastructure réseautique

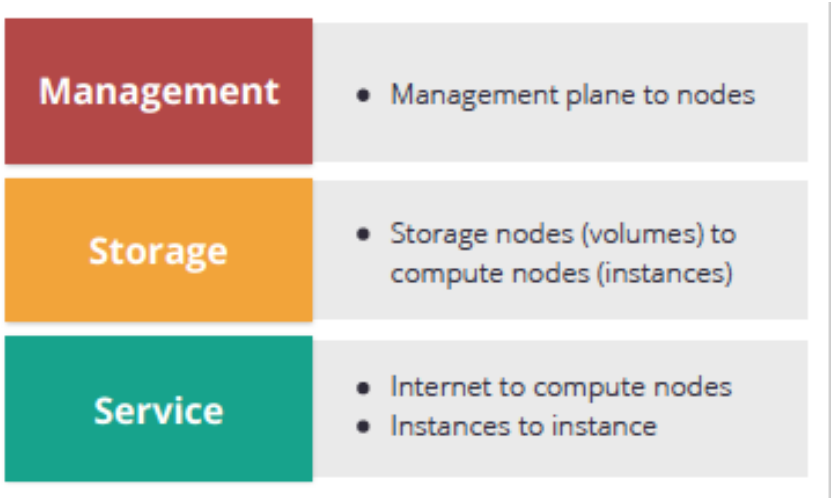
- L'infrastructure de base (stockage, réseautique, serveurs) pour soutenir l'infrastructure de virtualisation et l'arrière-boutique
- Abstraction de l'infrastructure réseautique
  - L'utilisateur est restreint à une définition virtuelle de composants réseautiques (*appliances* ou fonctions virtuelles)
  - Certains dispositifs ne lui sont pas disponibles directement *mais au travers d'un service*, ex: IDS/IPS

Technologies de la virtualisation réseautique

- *Abstraction du réseau*
  - *Virtual Local Area Network /* VLAN
    - Mécanisme de la couche 2 / réseau local du modèle OSI
    - Permet une ségrégation du trafic
    - N'est pas conçu pour le cloud mais très largement utilisé !
  - *Software Defined Networking /* SDN
    - Abstraction d'infrastructure réseautique d'un centre de données
    - Découplage du physique : *management plane & control plane & data plane*

L’infrastructure de base

- Constitué de 3 réseaux qui doivent être séparés et sécurisés
  - Management
    - Accès à la console et API
  - Stockage
    - Connexion du stockage aux machines virtuelles
  - Service
    - Communication des machines virtuelles entre elles et l’Internet



Éléments du domaine

- *Cloud compute & workload* et sécurité
- Appliance virtuelles
- *Software Defined Networking /* SDN
  - Routeur, coupe-feu, commutateur, serveur spécifique, dispositifs de sécurité : IDS/IPS, contrôle d'accès Internet, NGFW, WAF, etc
- *Software Defined Perimeter /* SDP
- Micro-segmentation
  - Principes Zero-Trust (non mentionné dans le document du CSA)

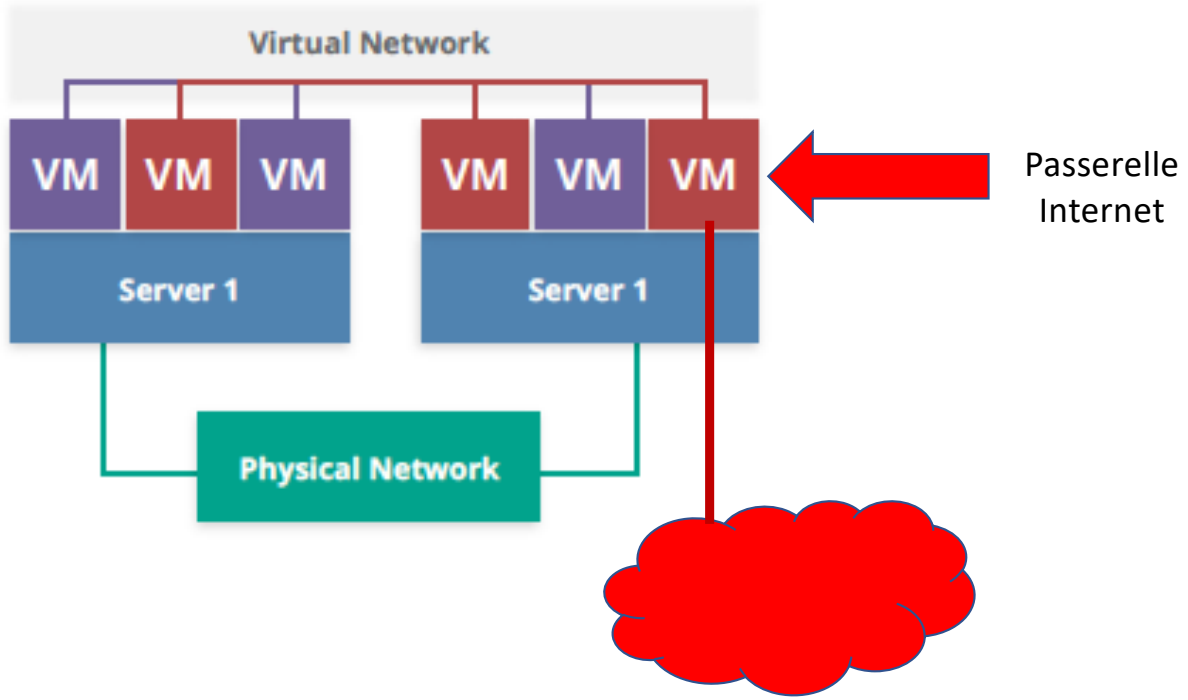
Cloud compute & workload et sécurité

- Malgré l'abstraction, le traitement dans le cloud s'exécute toujours sur du matériel
- Des mécanismes d'isolation et de contrôle doivent être en vigueur afin d'assurer la sécurité
  - Isolation
  - Supervision
  - Contrôle d'accès
- Ces mécanismes s'appliquent du *métal/microcode* jusqu'à la couche applicative et dans les niveaux d'abstraction
  - VM
  - Containeurs
  - *Serverless computing*

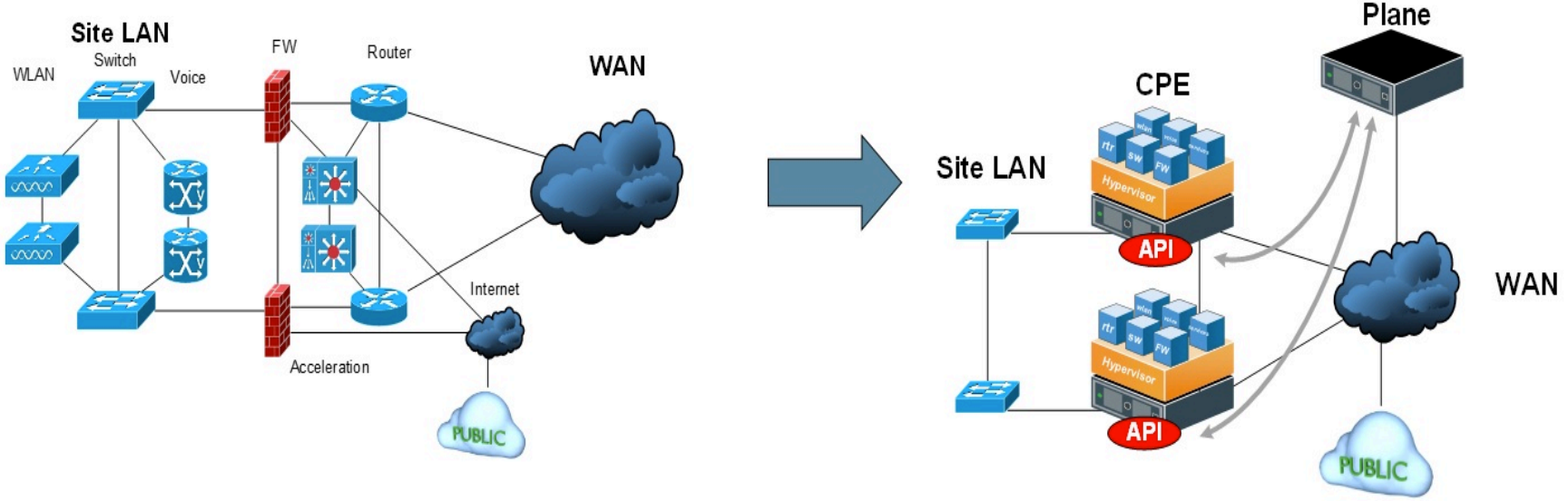
Appliance virtuelle

- Machine virtuelle préconfigurée, prête à l'exécution dans un hyperviseur/cloud
- Enjeux des appliances virtuelles
  - Peuvent devenir des goulots d'étranglement pour le trafic ou être bridés
  - Elles peuvent accaparer des ressources CPU et de mémoire
  - Elles doivent fonctionner en mode cloud (extensible, vélocité)
  - Doivent offrir de la résilience, support à du dynamisme (changement IP, éphémère)

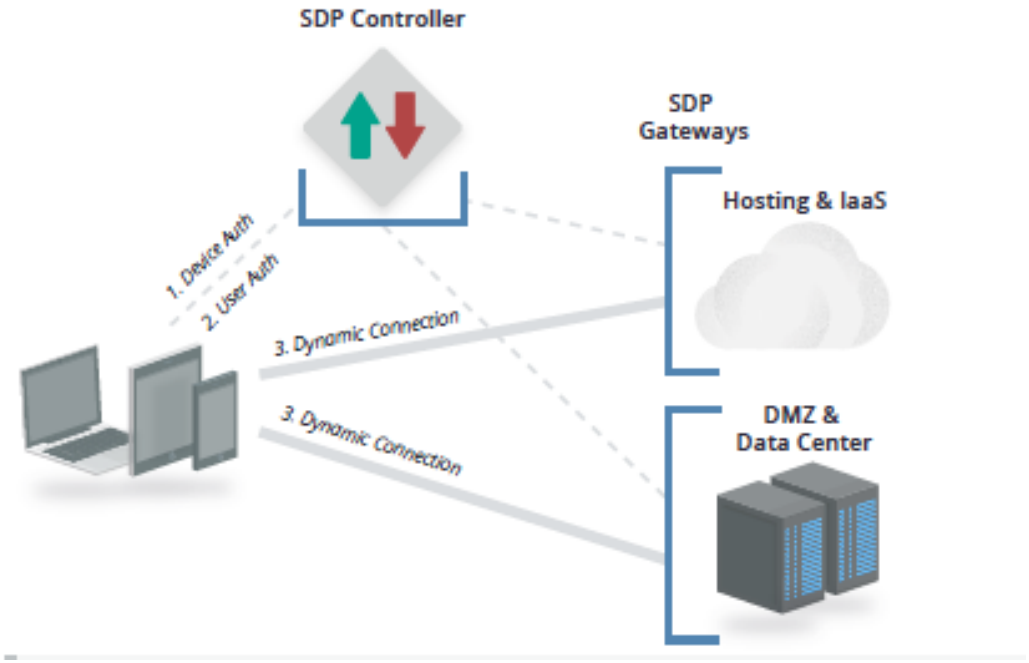
Exemple simplifié d'une appliance virtuelle



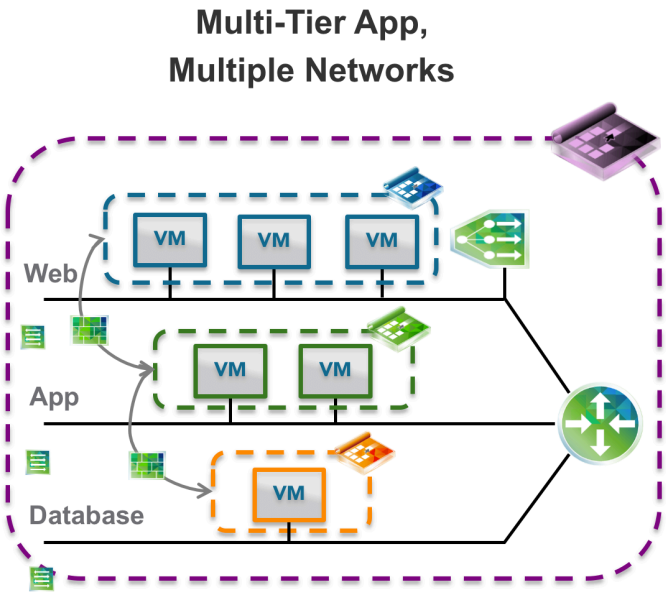
Réseau traditionnel et Software Defined Networking / SDN

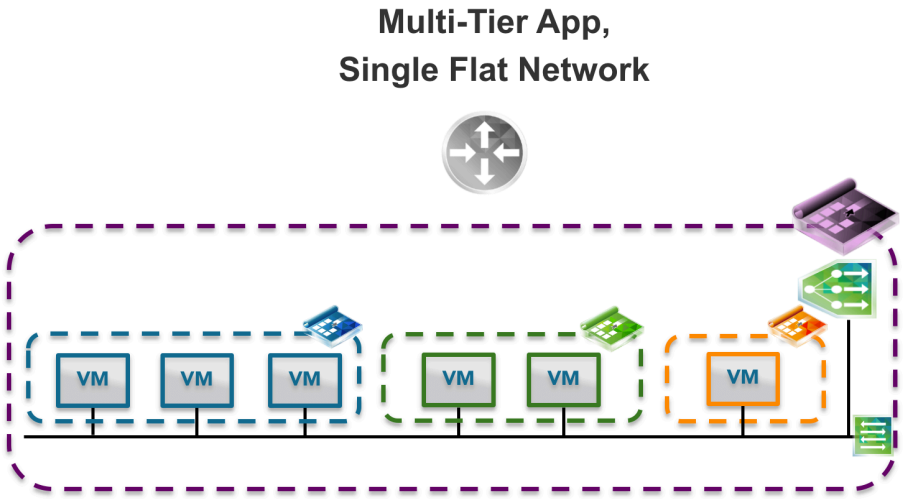


Software Defined Perimeter / SDP



Micro-segmentation





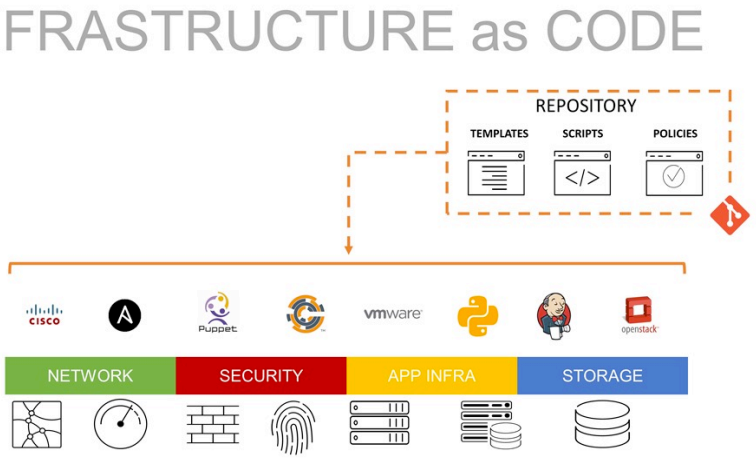
Notion de micro-périmètre

Principes du Zero-Trust

- Principes 0-Trust résumés sommairement :
  - Toutes les entités doivent être authentifiées
  - Toutes les entités (surtout les dispositifs) sont « sécurisées »
  - Les privilèges sont réduits au maximum
  - Contrôler les accès réseaux
    - Les mouvements latéraux non permis dans l'infrastructure réseau
    - Avoir la visibilité nécessaire
    - Visibilité et analyse de l'ensemble du trafic
    - La capacité de segmenter, isoler et contrôler le réseau d'une façon dynamique
- La mise en œuvre de « Zero-Trust » est grandement facilitée par l'utilisation de la technologie *Infrastructure as a Code*

Infrastructure as code / IaC

- Automatisation et orchestration d'une série d'étapes de configuration et de déploiement (provisionning et deprovisionning) d'environnements virtuels
- Infrastructure virtuelle qui est scriptée

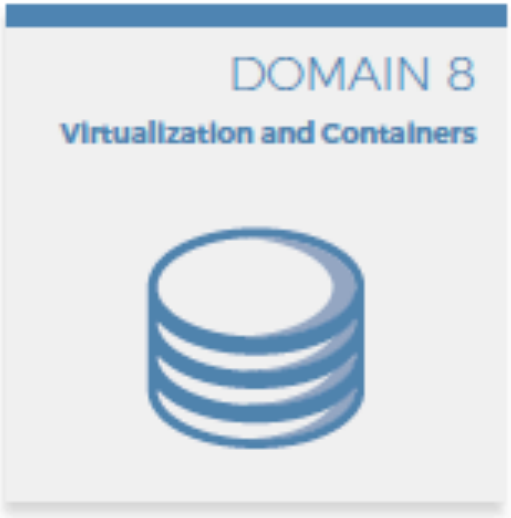


https://www.f5.com/company/blog/what-is-infrastructure-as-code-for-netops

Notion « *immutable workload* »

- Repose principalement sur la technologie des containeurs
  - Dynamique et extensible (*auto scaling*)
  - *Infrastructure as code* (IaC)
- L'utilisateur a peu ou pas de contrôle sur la localisation de l'exécution
- Le code est identique, peu importe l'environnement
- Repose sur une « image », l'exécution peut être interrompue et relancée
- *Serverless computing*

Domaine 8: Virtualisation et technologie des containeurs

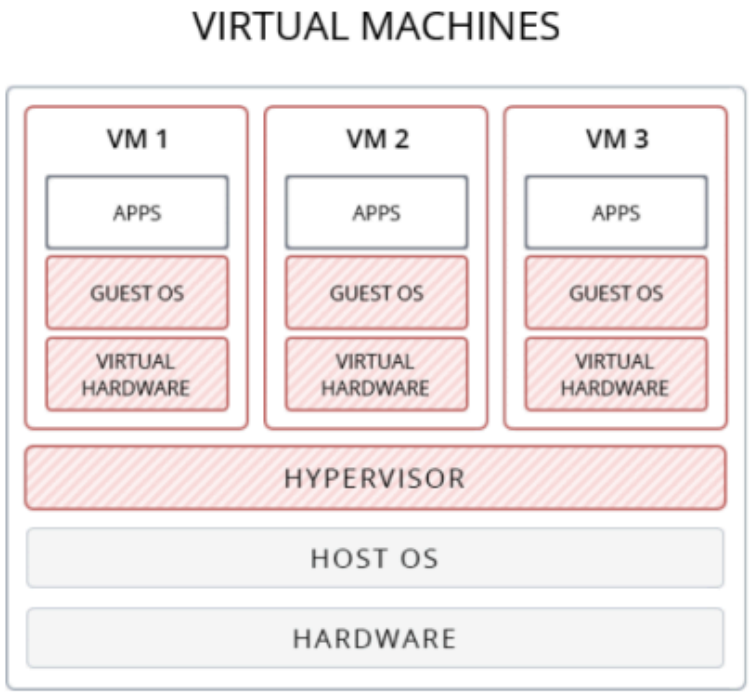


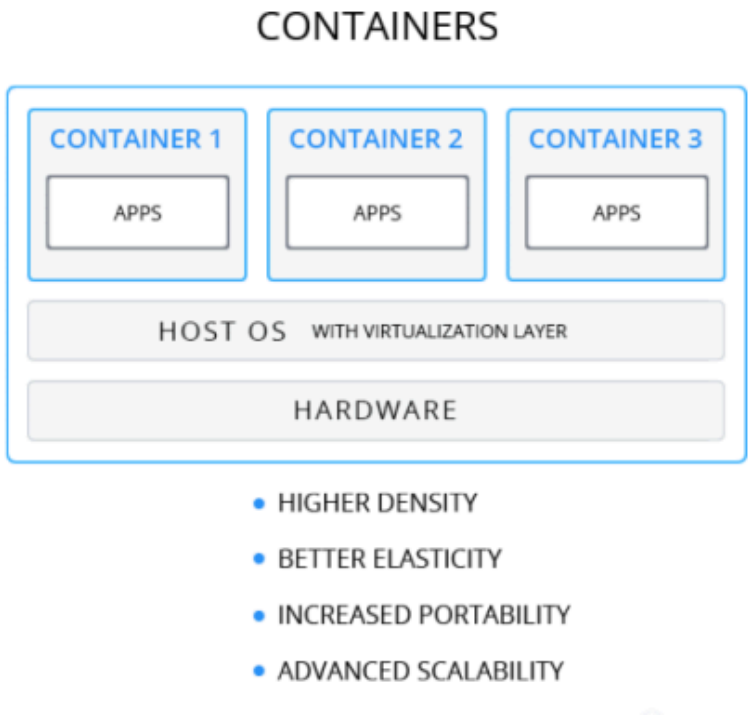
- Virtualisation
- Containeurs
- Orchestration

Virtualisation

- La virtualisation est une des briques fondatrices de l'infonuagique
- Notion de *pooling ressources, ressource pools*
- Les ressources se classent dans ces catégories :
  - Traitement, serveurs / *Compute*
  - Réseautique / *Network*
  - Stockage / *Storage*
  - Containeurs / *Containers*

Technologie des containeurs

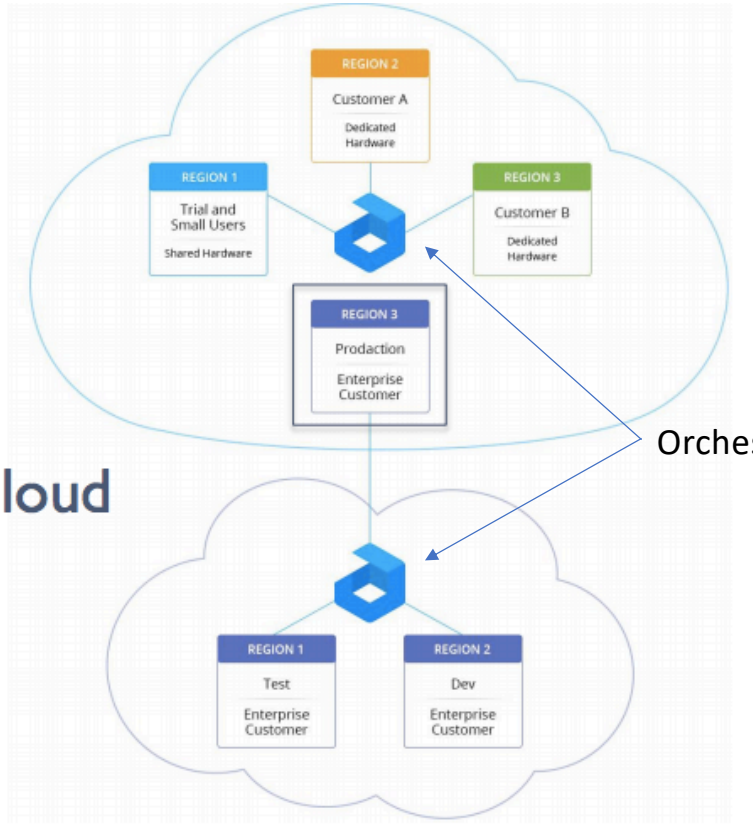




Éléments de la technologie des containeurs

Trois éléments clés

- Containeurs
  - Environnement d'exécution
- Orchestrateurs
  - Contrôleurs
- Répertoire ou Hub
  - Images, codes



Domaine 9: Réponse aux incidents

- Processus de détection, de réponse, de notification et de remédiation pour le consommateur et le prestataire du service

Cycle de vie de la réponse aux incidents

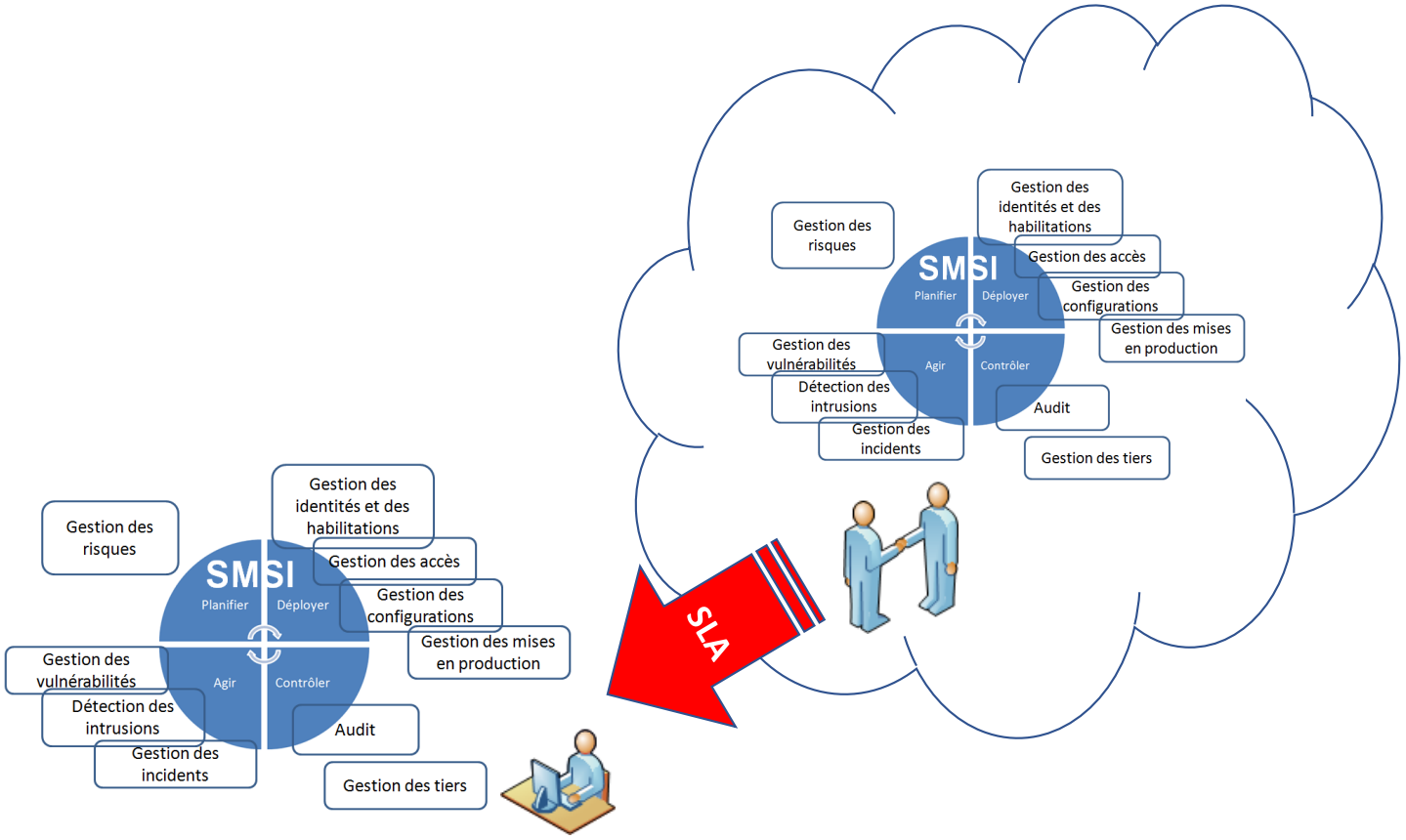
Basée sur NIST 800-61rev2

- Préparation / *Preparation*
  - Création du processus
  - Mise en place des ressources (humaines et matérielles)
  - Formation
- Détection et analyse / *Detection & Analysis*
  - Détection, alertage, évaluation, documentation, etc
- Circonscription, éradication et recouvrement / *Containment, Eradication, Recovery*
  - Circonscrire l'attaque, éradiquer le vecteur d'attaque, recouvrer les données, systèmes
  - Documenter l'incident
- *Post-Mortem*
  - Analyser et apporter les actions correctrices

Cloud et réponse aux incidents

- Préparation
  - Gouvernance et contrat/SLA, temps de réponse à un incident, qui contacter
  - Architecture : mesures de contrôle et outils
- Détection et analyse
  - Peut-être différent selon le type de service : IaaS != SaaS
  - Journaux, sources de données, mécanismes de détection
  - Enjeux de visibilité du réseau
  - Investigation et les outils forensiques
    - Images de serveurs ou disques, conservation de la preuve, etc
- Circonscription, éradication et recouvrement
  - IaaS - reconstruction à partir d'une image « propre »
  - PaaS, SaaS plus du ressort du fournisseur
- *Post-Mortem*
  - Collaboration entre l'équipe interne et celle du fournisseur

Lien entre les SMSI dans le cloud



Domaine 10: Sécurité applicative

- Sécurité application des applications développées et exécutées dans le nuage
- *Secure Software Development Lifecycle* / SSDLC

Développement et sécurité

- Qu'est-ce qui est différent dans le mode cloud versus le mode traditionnel ?
- Revoir les méthodologies et principes de développement en fonction du cloud
- Assurer la sécurité et la robustesse des applications

Opportunités

- Environnement de développement cloud sécuritaire
- Efficient et performant
- Environnement isolé
- Indépendance des plate-forme / machine virtuelle (micro service)
- Élasticité ou extensibilité
- Interface unifiée
- DevOps, DevSecOps

Enjeux

- Visibilité réduite
- Élargissement de la portée des actions des développeurs
- Changement du modèle des menaces
- Perte de transparence

Éléments du domaine

- *Architecture de développement*
- *Secure Software Development Lifecycle* / SSDLC
  - Microsoft's Security Development Lifecycle
  - NIST 800-64 *Security Considerations in the System Development Life Cycle*
  - ISO/IEC 27034 *Application security*
  - *Open Web Application Security Project* / OWASP
- DevOps & *Continuous Integration, continuous deployement* CI/CD
  - Livraison continue

Domaine 11: Sécurité des données et le chiffrement

- Protection de l'information, des données
- Mesure de contrôle : chiffrement
- Gestion des clés

Protection de l'information, des données

- Stockage des données dans le nuage
  - Architecture, contrôle d'accès, chiffrement, surveillance et alertage, tous autres moyens spécifiques
- Migration ou chargement des données
  - Déterminer quelles données vont dans le nuage (gouvernance)
- Chiffrer les données

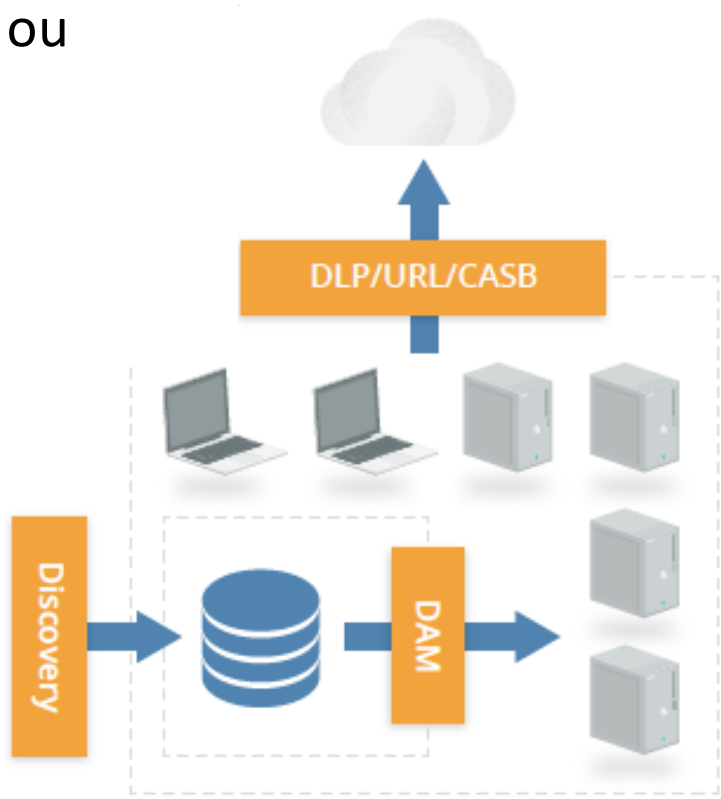
Types de stockage des données

- Les données sont stockées avec un de ces moyens :
  - Objets
    - Fichiers manipulés comme des objets, accessibles par des API
  - Volume
    - Fichiers pour les VM
  - Base de données
    - Relationnelle et non relationnelle
  - Applicatif / plate-forme
    - *Content Delivery Network* / CDN, fichiers dans un SaaS, cache, etc

- Les fournisseurs cloud utilisent parfois la technique de *Data Dispersion* ou *Data fragmentation of bit splitting*

Migration des données dans le nuage

- *Cloud Access and Security Brokers* / CASB ou Cloud Security Gateway
  - *URL filtering*
  - *Data Loss Prevention* / DLP
- *Database Activity Monitor* / DAM



Chiffrement des données

- Chiffrement
  - Le **chiffrement** ou **cryptage** est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel. (wikipedia)

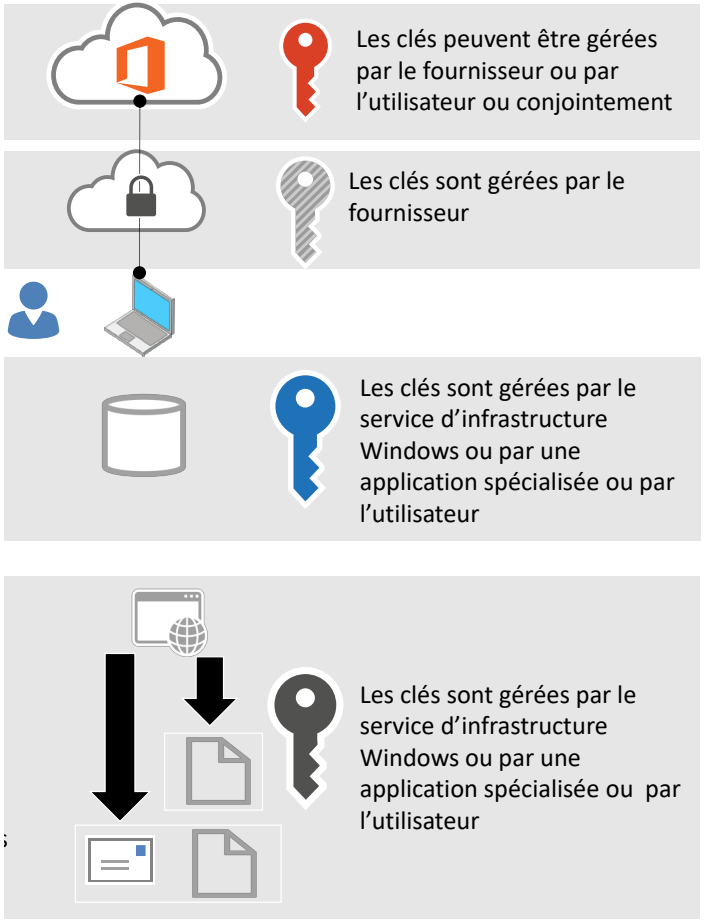
- *Et Tokenization*
  - … la **tokenisation** est le procédé permettant de remplacer une donnée critique par un élément équivalent qui n'aura aucune valeur intrinsèque ou signification exploitable une fois sortie du système. (wikipedia)

Le chiffrement dans le nuage : Facile à dire …

- Trois composants
  - Les données
  - L'engin de chiffrement
  - La gestion des clés
- La question de la gestion des clés est majeure
  - Localisation des clés
  - Qui les détient ? Le fournisseur, avez-vous confiance en lui ?
  - La pérennité des clés

Chiffrement et infonuagique

- Le chiffrement intervient sur plusieurs couches technologiques lors de la consommation de services infonuagiques



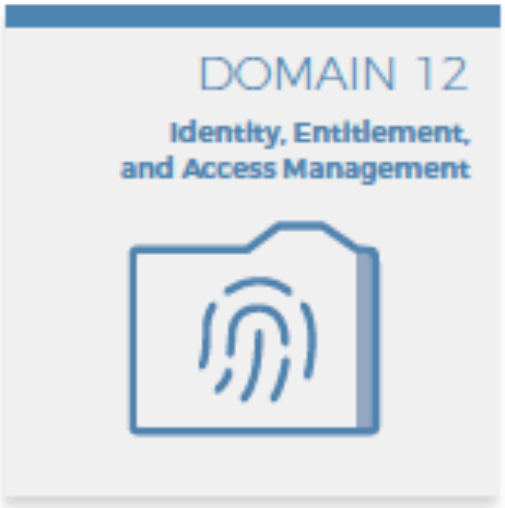
Scénarios de gestion des clés

	Gérer les clés localement	Gérer les clés dans le nuage	Gérer par le fournisseur
Exemple dans Microsoft Azure	**(Customer Managed Keys - Hold Your Own Key)** Le client héberge, produit et gère les clés.	**((Customer Managed Keys in Azure Key Vault)** Le client produit et gère les clés dans une voûte sécurisée dans le nuage de Microsoft	**(Microsoft Managed Keys)** Microsoft héberge, produit et gère les clés
Principaux enjeux	Certains services avancées ne sont pas disponibles. Les données sont opaques pour les services infonuagique : pas d'antivirus, de recherche, protection contres les fuites de données.	La clé maitresse est contrôlée par le contrôleur des clés de l'organisation. *Cependant, une clé maitresse de secours (Availability Key) est détenue par Microsoft.*	La gestion des clés est réalisée par Microsoft. Cependant des mécanismes stricts contrôlent l'accès aux clés par le fournisseur.
Qui gère les clés de chiffrement ?	Les clés de chiffrement sont détenues et contrôlées par le client.	Les clés de chiffrement sont contrôlées par le client mais elles résident dans une voute sécurisée dans le nuage.	Les clés de chiffrement sont détenues et contrôlées par le fournisseur.

Dispositifs de gestion des clés

- *Hardware Security Module* / HSM
  - Sous le format d'une *appliance* matériel
- *Virtual appliance*
  - *Logiciel qui joue le rôle de HSM*
- *Cloud provider service*
  - Service de gestion de clés offert par un service cloud
- Hybride
  - Combinaison de HSM et de logiciel ou service

Domaine 12: Gestion des identités, des accès et des habilitations



- Service de répertoire pour les besoins de gestion des identités et des accès en des habilitations ou des droits (IdEA)
- Extension d’un répertoire d’entreprise

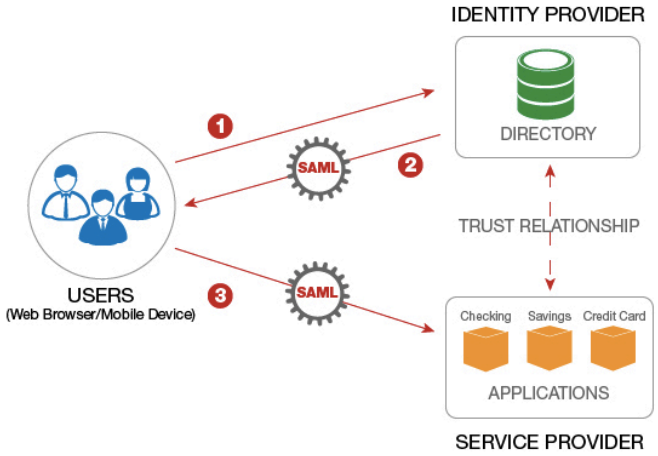
État des lieux

- *Identity and Access Management* / IAM
  - Moyen de donner à une entité, l'accès aux ressources auxquelles elle a droit au bon moment et pour les bonnes raisons
- Domaine compliqué et complexe
  - Plusieurs identités, plusieurs systèmes différents, plusieurs fournisseurs
- La solution est la fédération mais elle exige des normes, de la sécurisation et du maintien

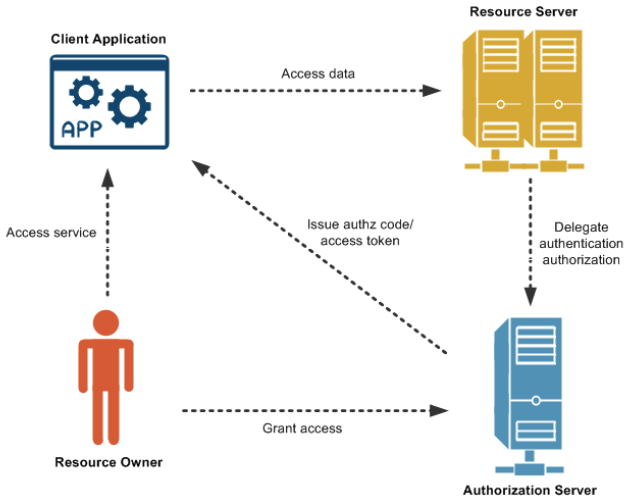
Terminologie

- *Entity* / Entité
- *Identity* / Identité
- *Identifier* / Identifiant
- Attribut
- Personna
- *Role* / Rôle
- *Authentication* / Authentification
- Authentification forte *ou Multifactor Authentification* / MFA
- *Access control* / Contrôle d'accès
- *Authorization* / Autorisation
- *Entitlement /Droit d'accès*
- *Federated Identity Management*
- *Autoritative source*
- *Identity provider /* Courtier d'identité
- *Relying Party*
- *Single Sign On / SSO*

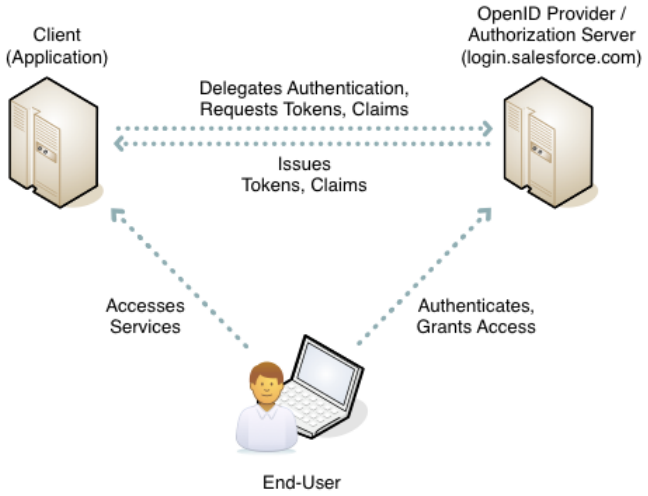
Normes



Security Assertion Markup Language 2.0
SAML



Oauth 2.0



OpenID
(basé sur Oauth)

Protocol : SAML vs OAuth 2.0 vs OpenID

(SAML)

- Federated Identity
  - Who are you ?
  - Permission : Allow/ Denied
- OASIS/WS-*
- SAML Assertion
  - 1.0, 1.1, 2.0
  - XML based
  - Signed/Encrypted

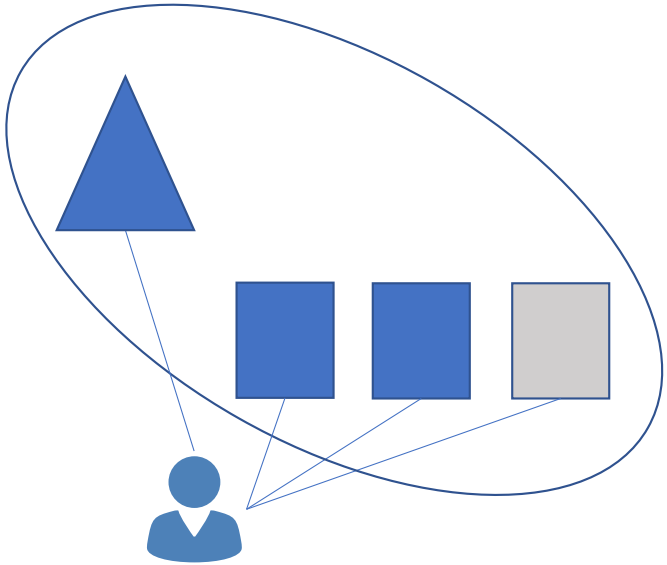
- Delegated authorization
  - Permission : Allow/ Denied
- IETF RFC 6749
- access_token (RFC6750)
  - Bearer *
    - Vendor specified
  - Introspection : IETF RFC 7662

OpenID®

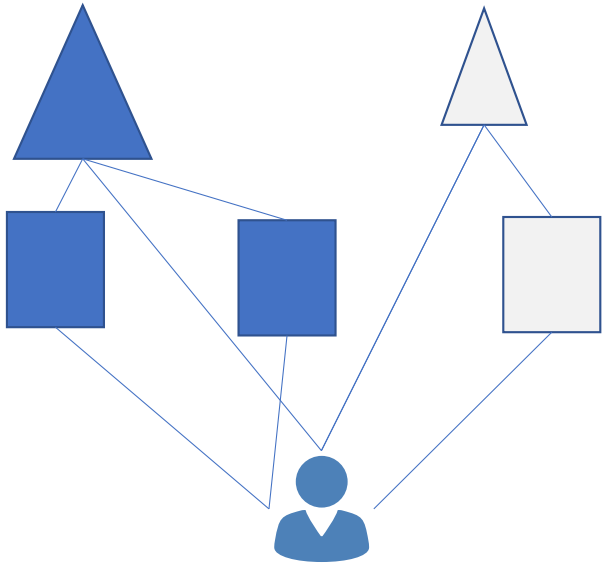
- Authentication
  - Who are you ?
- OpenID.net
- Extend OAuth 2.0 with user information
- id_token
  - JSON Web Token (JWT)
    - Signed with JWS
    - Encrypted with JWE
    - Signed & Encrypted

Extrait du document *Token OAuth/OIDC/JWT/SAML,* shiufun@us.ibm.com, STSM, Security, APIc/GW, Cloud Division

Fédération et forme libre



SAML



OpenID
0Auth

Domaine 13: SecaaS / Security as a Service

- Services infonuagiques pour les besoins de sécurité, gestion des incidents, vérification de la conformité et audit, gestion des identités et des accès

Bénéfices

- Pallier aux manque de ressources humaines et d'expertise
- Partage d'information et de connaissance (*Intelligence*)
- Flexibilité de déploiement
- Isolation du client
  - La menace est mitigée avant d'atteindre le client
- Extensibilité, à la demande et contrôle des coûts
  - *Pay as you grow*

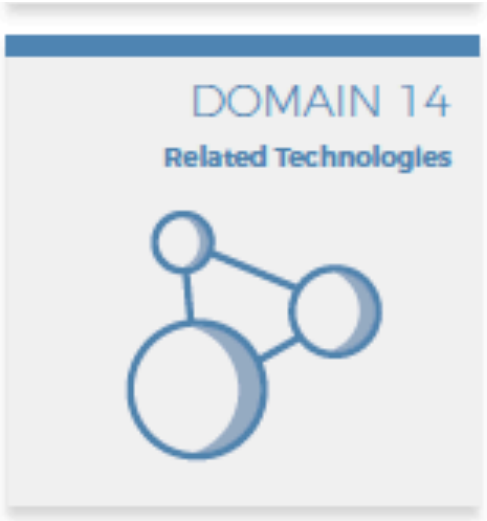
Préoccupations

- Manque de visibilité
- Législations différentes qui peuvent s'appliquer
- Manipulation des données selon des législations différentes
- Fuite de données
- Migration du traditionnel vers le SecaaS
- Changement de fournisseurs

Les services SecaaS

- Identity, Entitlement and Access Management Services / Gestion des identités, accès et habilitations
  - *Identity as a Service*
- *Cloud Access and Security Brokers / CASB*
  - *Cloud Security Gateway*
  - Services génériques
- *Web Security / Web Security Gateways*
- *Email Security*
- *Security Assessment*
- *Web Application Firewall / WAF*
- *Intrusion Detection Prevention / IDS/IPS*
- *Security Information & Event Management / SIEM*
- Encryption & Key Management / Service de chiffrement ou Gestion des clés
- *Business Continuity & Disaster Recovery*
- *Security Management*
- *Distributed Denial of Service Protection*

Domaine 14: Technologies associées



- Ce sont des technologies établies ou émergentes qui reposent en tout ou en forte partie sur l'infonuagique

Quels sont ces technologies ?

- *Big Data /* Données massives
- IoT / Internet des objets
- Dispositifs mobiles
- *Serverless computing*
- *Éventuellement*
  - *Blockchain as a Service / BaaS*

Big Data / Données massives

- Ensemble de technologies et de techniques pour manipuler et traiter de très gros volume de données
- 3 « V » : *High Volume, High Velocity, High Variety*
- *Cloud et Big Data*
  - *Distributed data collection*
  - *Distributed storage*
  - *Distributed processing*

Enjeux du Big Data

- Considérations de sécurité et vie privée
- Protection des données (data collection)
- Gestion des clés de chiffrement
- Robustesse des mécanismes de sécurité
- Gestion des accès et des habilitations
- PaaS
  - Effets collatéraux de certains services PaaS tel que le *machine learning*

IoT / Internet des objets

- L'Internet des objets désigne les objets physiques dotés de capacité de traitement de l'information et d'une connectivité réseau permettant de communiquer avec d'autres entités (objets, réseaux, services ou humains)

  « The "Internet of Things" refers to physical objects that have embedded network and computing elements and communicate with other objects over a network. »

  Internet of things, risk and value considerations, ISACA

Enjeux de l'IoT

- Gestion des mise à jour et des correctifs des objets
- Cycle de vie des objets : enregistrement, authentification, habilitation
- Sécurité des API
- Sécurité et sanité des données
- Chiffrement des données et des communications

Mobile computing ou Mobilité

- La mobilité n'est pas exclusive au cloud et même plus vieille que le cloud
- L'arrière-boutique ou *backend* est souvent dans le cloud
- Les enjeux sont identiques à ceux de l'IoT

Serverless computing

- Un autre *buzzword* ?
- Le *Serverless computing* désigne l'utilisation optimum des services PaaS dans l'environnement du fournisseur cloud sans aucune gestion de plateforme ou même de containeurs
- Dématérialisation et abstraction
  - Stockage d'objets, balanceurs de charge, base de données, *machine learning, message queuing,* service de notification/alertage, API, serveur web

Enjeux du *Serverless computing*

- Sécurité du fournisseur de service : SLA et capacité de réaliser
- Accès à des outils ou informations de sécurité de plus haut niveau avec moins de détail ou information
- Conformité et audits ne sont pas forcément uniforme sur l'ensemble des services exploités
- Toute la gestion se réalise au travers de la console de gestion
- Réduction de la surface d'attaque
- Balayage des vulnérabilités et gestion des incidents sont plus difficiles

Cloud Computing,
BENEFITS, RISKS AND
RECOMMENDATIONS FOR INFORMATION SECURITY

https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file

CLOUD COMPUTING, BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY

- Document très dense
- Propose une analyse complète des risques du cloud

R.1 LOCK-IN

Probability	HIGH	Comparative: Higher
Impact	MEDIUM	Comparative: Equal
Vulnerabilities	V13. Lack of standard technologies and solutions V46. Poor provider selection V47. Lack of supplier redundancy V31. Lack of completeness and transparency in terms of use	
Affected assets	A1. Company reputation A5. Personal sensitive data A6. Personal data A7. Personal data - critical A9. Service delivery – real time services A10. Service delivery	
Risk	**HIGH**	

2. Risk assessment

- *Use-case scenarios*
  - *SME migration to cloud computing services*
  - *the impact of cloud computing on service resilience*
  - *cloud computing in e-Government (e.g., eHealth)*
- *Risk assessment process*

Cartographie des risques

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

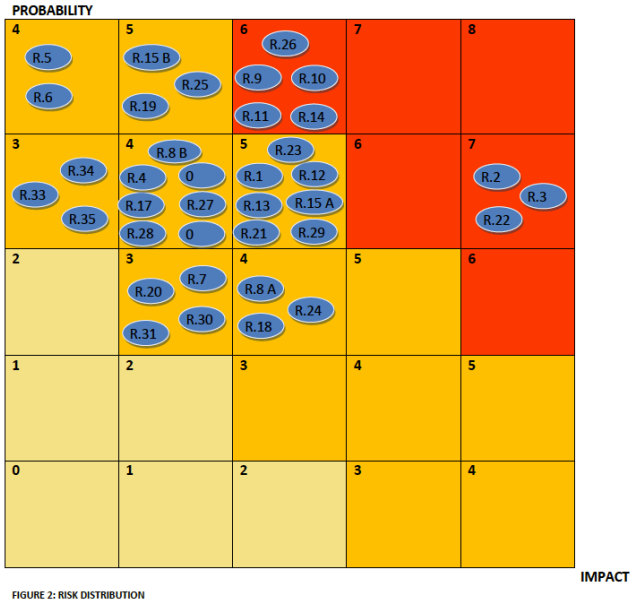


FIGURE 2: RISK DISTRIBUTION

3. Risks
Policy and organizational risks

- *R.1 Lock-in*
- *R.2 Loss of governance*
- *R.3 Compliance challenges*
- *R.4 Loss of business reputation due to co-tenant activities*
- *R.5 Cloud service termination or failure*
- *R.6 Cloud provider acquisition*
- *R.7 Supply chain failure*

Technical risks

- *R.8 Resource exhaustion (under or over provisioning)*
- *R.9 Isolation failure*
- *R.10 Cloud provider malicious insider - abuse of high privilege roles*
- *R.11 Management interface compromise (manipulation, availability of infrastructure)*
- *R.12 Intercepting data in transit*
- *R.13 Data leakage on up/download, intra-cloud*
- *R.14 Insecure or ineffective deletion of data*
- *R.15 Distributed denial of service (DDoS)*
- *R.16 Economic denial of service (EDOS)*
- *R.17 Loss of encryption keys*
- *R.18 Undertaking malicious probes or scans*
- *R.19 Compromise service engine*
- *R.20 Conflicts between customer hardening procedures and cloud environment*

Legal risks

- *R.21 Subpoena and e-discovery*
- *R.22 Risk from changes of jurisdiction*
- *R.23 Data protection risks*
- *R.24 Licensing risks*

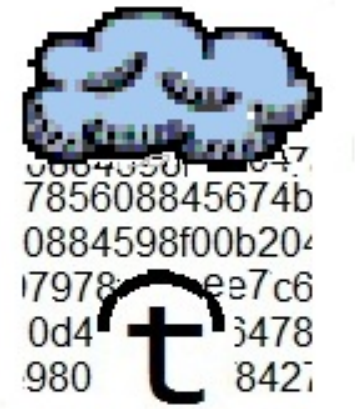
Risks not specific to the cloud

- *R.25 Network breaks*
- *R.26 Network management (ie, network congestion / mis-connection / non-optimal use)*
- *R.27 Modifying network traffic*
- *R.28 Privilege escalation*
- *R.29 Social engineering attacks (ie, impersonation)*
- *R.30 Loss or compromise of operational logs*
- *R.31 Loss or compromise of security logs (manipulation of forensic investigation)*
- *R.32 Backups lost, stolen*
- *R.33 Unauthorized access to premises (including physical access to machines and other facilities)*
- *R.34 Theft of computer equipment*
- *R.35 Natural disasters*

Autres sections

- *4. Vulnerabilities*
  - *Vulnerabilities not specific to the cloud*
- *5. Assets*
- *6. Recommendations and key messages*
  - *Information assurance framework*
  - *Information assurance requirements*

Merci de votre attention



Tactika inc.

clement.gagnon@tactika.com

www.tactika.com

@tactika

http://ca.linkedin.com/in/tactika