Plan d'Assurance Sécurité

ORANGE BUSINESS

CLOUD AVENUE

Version : 1.3
Date : 26/11/2024

Business

Description du document

Propriétés				
Titre document	Plan d'Assurance Sécurité – Cloud Avenue			
Version	1.3			
Rédacteur	Business Security Officer (BSO) Cloud Avenue			
Statut	❑ En cours	❑ Revue	■ Validé	❑ Approuvé
Date	mardi 26 novembre 2024			

Classification du document

Classification	
Confidentialité	Sans restriction

Diffusion

Société	Fonction	Diffusion
Global Delivery & Operations (GDO)Sales		Lecture
	BM-GDO Sales	Approbation
		Lecture
Orange Business/Global Delivery & Operations (GDO)/ Global Platforms & Service (GPS)	Chief Information Security Officer (CISO) GDO/GPS	Lecture
	BSO Cloud Avenue	Rédaction

Historique des versions

Version	Opération	Nom	Date
1	Création du document	OCB Sales	Septembre 2020
2	Revue des Indicateurs et de la RACI	OCB Sales	Mars 2021
3	Mise à jour chap. 3	BSO Cloud Avenue	Septembre 2022
4	Mise à jour chap. 4	BSO Cloud Avenue	Décembre 2022
5	Changement de template	BSO Cloud Avenue	Janvier 2023
6	Rajout VCoD (chap. 4)	BSO Cloud Avenue	Mars 2023

Version	Opération	Nom	Date
7	Release version 1.0	BSO Cloud Avenue	Avril 2023
8	Remplacement OBS par OS	BSO Cloud Avenue	Novembre 2023
9	Mise à jour annuel	BSO Cloud Avenue	Janvier 2024
10	Changement marquage	BSO Cloud Avenue	Février 2024
11	Prise en compte HDS	BSO Cloud Avenue	Octobre 2024
12	Changement acronyme interne	BSO Cloud Avenue	Novembre 2024

Sommaire

Plan d'Assurance Sécurité (PAS)

1

INTRODUCTION

1.1. Objet du document

Le présent document constitue le Plan d'Assurance Sécurité (PAS) d'Orange Business pour la fourniture du service Cloud Avenue. Il décrit les principales mesures de sécurité techniques et organisationnelles appliquées par Orange Business pour garantir la sécurité de ses offres.

La prestation d'Orange Business pour Cloud Avenue est assurée par la division suivante d'Orange Business :

- Global Platforms and Services

Ce document s'applique aux offres Cloud professionnelles commercialisées par Orange Business à destination des entreprises. Les offres traitées dans ce document sont :

- Cloud Avenue

Le plan d'assurance sécurité est garant de la qualité de service en matière de sécurité entre Global Platforms and Services et Cloud Avenue.

1.2. Organisation du document

Le présent document est organisé autour des chapitres suivants :

- Le chapitre 1 constitue l'introduction du document ;
- Le chapitre 2 constitue une synthèse des atouts de Cloud Avenue sur les aspects sécurité ;
- Le chapitre 3 liste les mesures de sécurité mises en œuvre, organisées selon les thématiques de l'ISO 27002 ;
- Le chapitre 4 détaille les mesures de sécurité complémentaires spécifiques à chaque offre ;
- Les annexes.

II

SYNTHÈSE : SÉCURITÉ CLOUD

Forces des offres Cloud d'Orange sur la sécurité

Localisation des données : Orange Business garantit la localisation des données et sauvegardes des clients dans un ou des pays donné(s).

Sécurité physique des centres d'hébergement : tous les centres

Sécurité du portail d'administration : les clients disposent de portails leur permettant de gérer leurs offres Cloud. L'accès à ces portails s'effectue avec des comptes nominatifs, les actions y sont journalisées, et les échanges sont protégés et chiffrés. La sécurité des portails est contrôlée régulièrement avec des tests d'intrusion.

Connectivité avec les VPN entreprises : les environnements virtualisés des clients Cloud peuvent être interconnectés de manière sécurisée avec les VPN MPLS entreprises (« Business VPN »), assurant l'isolation réseau de bout en bout, ainsi qu'une bande passante et une qualité de service réseau que ne peut pas garantir Internet.

d'hébergement sont certifiés ISAE 3402[1] Type II (ex SAS 70) et sont de niveau équivalent TIER III ou TIER IV. Comme précisé en annexe A, TIER III et TIER IV sont les deux niveaux les plus performants de la classification TIER.

L'expérience de l'opérateur : L'environnement Cloud Avenue a conçu en se basant sur l'expérience d'Orange en tant qu'opérateur d'infrastructure critique et en tant qu'un des leaders français dans l'intégration et le conseil en sécurité (Orange Cyberdefense).

Sécurité des opérations de support et de maintenance : les centres d'exploitation sont situés en France et à l'étranger et disposent de la certification sécurité ISO 27001 [2] , de manière à assurer la confidentialité des informations des clients Orange. Nos exploitants sont sensibilisés aux bonnes pratiques de sécurité et accèdent de manière sécurisée aux plateformes Cloud : comptes nominatifs, traçabilité de leurs actions et chiffrement des flux d'administration.

Protection contre les dénis de service [3] (DOS) : les offres Cloud Orange bénéficient d'un système de protection contre les attaques massives en déni de service provenant d'Internet. Il est déployé au cœur du réseau opérateur du Groupe Orange et s'appuie sur des équipements de sécurité spécifiquement conçus à cet effet.

Ce chapitre liste les principaux atouts des offres Cloud d'Orange Business sur les aspects sécurité

[1] ISAE 3402 : ISAE 3402 est un standard permettant aux clients de prestations externalisées d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de services. La norme traite en particulier la sécurité physique des centres d'hébergement.
[2] Certificat associé : https://certificats-attestations.afnor.org/certification=335181233155
[3] Les dénis de service : connus sous l'abréviation DOS (Denial Of Service) en anglais.

Sécurité du portail d'administration : les clients disposent de portails leur permettant de gérer leur organisation sur Cloud Avenue. L'accès à ces portails s'effectue avec des comptes nominatifs, les actions y sont journalisées, et les échanges sont protégés et chiffrés. La sécurité des portails est contrôlée régulièrement avec des tests d'intrusion.

Continuité de services des offres Cloud Orange : Cloud Avenue s'engage sur un taux de disponibilité du service élevé (se conférer aux descriptions de service). D'autre part, Cloud Avenue a une infrastructure entièrement redondée, avec des mécanismes de haute disponibilité de manière à rendre transparent les pannes locales : réseau (accès Internet, accès VPN, pare-feu), portail d'administration, virtualisation, stockage…

III

MESURES DE SÉCURITÉ

Mesures de sécurité communes

Les mesures de sécurité sont organisées en 14 chapitres, correspondant aux **14 chapitres de la norme ISO 27002 version 2017**.

3.1. Politique de sécurité

Ce chapitre correspond à la thématique 5 de l'ISO 27002 version 2017.

L'offre de Cloud Avenue suit les politiques de sécurité et réglementations suivantes

- **Politique de Sécurité Globale** (PSG) du groupe Orange
  - Langue : français
  - Validation : PDG du Groupe Orange
  - Référence : « PSG O.2017D005 Ed3 – 22 Septembre 2017* [1]»
- **Politique de Sécurité sectorielle** Orange Business
  - Langue : anglais
  - Validation : Vice-président Exécutif d'Orange Business
  - Référence : « OBS Sectorial Global Security Policy V 20.2* - 20 Oct 2022 [2] »
- **Politique de Sécurité** de Global Delivery & Operations
  - Langue : anglais
  - Validation : Directeur de Global Delivery & Operations
  - Référence : « Global Platforms & Services Cloud Security Policy V 1.14* - 18 Oct 2024 »
- **Politique de Management des vulnérabilités** d'Orange Cloud for Business
  - Langue : Anglais
  - Validation : CISO Orange Business
  - Référence : « Technical vulnerability management v1.6 [4] »
- **Politique de sécurité des réseaux** de Global Delivery & Operations
  - Langue : Anglais
  - Validation : CISO Orange Business
  - Référence : « Network_Security_Policy_3.0_juin2020 [5] »
- **Politique de Management des incidents** de Sécurité de Global Delivery & Operations
  - Langue : Anglais
  - Validation : CISO Orange Business
  - Référence : « security_incident_management_policy_and_proceduresv1.6 [6] »
- **Réglement Générale de Protection des Données (GDPR)**
  - Langue : Anglais
  - Référence : https://gdpr-info.eu/

- **Hébergement de Données de Santé (HDS)**
  - Langue : Français
  - Référence : https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel_certification_hds---fr--v2.pdf

**Ces documents sont confidentiels, mais consultables partiellement dans les locaux d'Orange après signature d'un engagement de confidentialité.*

Ces politiques sont alignées sur les normes ISO 27001 et ISO 27002 relatives à la sécurité des systèmes d'information.

3.2. Organisation de la sécurité

Ce chapitre correspond à la thématique 6 de l'ISO 27002 version 2017.

Cette partie décrit d'un point de vue « sécurité » l'organisation de l'offre Cloud Avenue.

Organisation sécurité de l'offre Cloud Avenue

3.2.1. Direction Sécurité d'Orange

La Direction de la Sécurité d'Orange (DSEC), rattachée au Secrétariat Général du Groupe, anime et coordonne les actions de sécurité sur l'ensemble du périmètre du Groupe Orange. Ses missions sont les suivantes :

- Définition des Politiques de Sécurité (générale, sectorielle) ;
- Définition des politiques de sensibilisation et de formation du personnel à la sécurité, promotion de la sécurité dans la stratégie et la culture de l'entreprise ;
- Interface avec certains organismes ayant des activités de sécurité :
  - La Défense Nationale et les autorités gouvernementales (SGDN, DCSSI, …) ;
  - Les autorités de justice, de police et de gendarmerie (en liaison avec la Direction Juridique d'Orange) ;
  - La CNIL (en liaison avec la Direction Juridique et le Secrétariat Général d'Orange) ;
  - La Direction de l'Audit et du Contrôle des Risques (DACR) d'Orange, le Centre National de Sécurité du Système d'Information (entité d'Orange) ;
  - Les CERT (Computer Emergency Response Teams), en particulier le CERT-IST.
- Centralisation des informations sur les incidents de sécurité, consolidation des données de tableau de bord émises par les différentes entités ;
- Pilotage des programmes de certification sécurité, comme la certification ISO27001 ;
- Réalisation d'audits et de contrôles, suivi des audits et contrôles réalisés à l'initiative des entités.

Le Business Security Officer transmet à Cloud Avenue toutes les requêtes des autorités.

3.2.2. Direction Sécurité Orange Cloud for Business

La direction de la sécurité de Global Delivery & Operations assure la bonne prise en compte de la sécurité dans l'ensemble des offres Cloud d'Orange. Ses missions sont par exemple :

- Définir la politique de sécurité et les guidelines à appliquer sur les offres Cloud ;
- Réaliser et mettre à jour les analyses de risques de sécurité (type ISO 27005) sur les offres Cloud ;
- Piloter les plans d'actions sécurité découlant de l'analyse de risques ;
- Garantir l'homogénéité des solutions de sécurité mises en place afin d'assurer leur effectivité et leur pérennité ;
- Capitaliser les connaissances d'Orange concernant la sécurité du Cloud ;
- Soutenir, conseiller, fournir de l'expertise sur les questions de sécurité du Cloud ;
- Former et sensibiliser le personnel aux procédures de sécurité ;

- Réaliser de la veille sécurité et travailler avec des instances internationales concernant la sécurité du Cloud. Orange Business participe ainsi à la Cloud Security Alliance[4] (CSA), l'ITU-T et l'ISO ; et intervient au niveau Européen en tant que membre du Cloud Security Expert Group de l'ENISA[5].
- Contrôler le niveau de sécurité des offres, par la conduite d'audits de sécurité réguliers (internes et/ou externes).

La direction est pilotée par le « Chief Security Officer » et est constituée des fonctions suivantes :

- Sécurité de l'ingénierie : en charge de piloter la sécurité lors de la conception de l'offre dans sa phase projet (définition de l'architecture, sécurisation des composants…). Contribution à la validation de la documentation projet (description de service, dossier d'architecture, recettes, procédures…). Intervention également en tant qu'expert sécurité tout au long du cycle de vie de l'offre (support niveau 3) ;
- Sécurité des Opérations : en charge d'assurer le maintien en condition de sécurité de l'offre. Expertise sécurité sur les évolutions menées sur les plates-formes. Traitement des incidents de sécurité et contrôle du respect du processus de gestion des vulnérabilités ;
- La mise à jour des documents de sécurité.

3.2.3. Business Security Officer

Dans le cadre de la prestation supplémentaire délivrée par Orange Cloud for Business, un Business Security Officer - BSO est nommé pour le client pour assurer le management de la sécurité tout au long de la prestation.

Par défaut, ses missions sont :

- Un contact privilégié au sein du département sécurité client de Global Delivery & Operations avec un Business Security Officer pour le suivi de la sécurité de la prestation et les conseils sécurité ;
- La collecte d'indicateurs de sécurité prédéfinis et un reporting périodique sous forme de tableau de bord sécurité et d'une réunion téléphonique ;
- Apporte sa contribution pour la coordination et la priorisation des actions de correction des incidents de sécurité ;
- Accompagne l'infrastructure lors de ses audits et suit les plans d'actions de correction ;
- La mise à jour annuelle de la documentation sécurité et d'un Plan d'Assurance Sécurité personnalisé.

---

[4] Cloud Security Alliance (CSA) : https://cloudsecurityalliance.org/

[5] ENISA : European Union Agency for Network and Information Security (ENISA) - www.enisa.europa.eu

Le Business Security Officer, dans le cadre de sa relation avec Cloud Avenue, s'assure du respect de la ségrégation des tâches et de la bonne application de la politique du SMSI et fournira ainsi les indicateurs correspondants. Il respecte et est garant des mesures de sécurité de l'information mises en œuvre au cours de la prestation. Il prend en compte dans son analyse les exigences du client et les spécificités réglementaires (certification HDS, GDPR) pour proposer d'éventuels ajustements voire de nouveaux services.

Les missions du Business Security Officer peuvent être étendues en fonction des prestations contractualisées (fréquence de reporting, indicateurs du tableau de bord, fréquence des audits, de la mise à jour de la documentation sécurité, gestion de la sécurité d'infrastructure dédiée telle que des locaux, IT et personnels dédiés etc.)

3.2.3.1. Comités de sécurité

Le « Comité Sécurité » est une instance qui permet de suivre régulièrement l'avancement du niveau de sécurité de la solution client. Il est organisé et animé par le Business Security Officer.

SW01 - COSEC (Comité de sécurité)		
Périmètre de la prestation couvert	Ensemble de la prestation	
Ordre du jour type	Pour la période écoulée ▪ Revue des alertes de sécurité ▪ Revue des indicateurs de sécurité ▪ Revue du PAS	
Fréquence	1 COSEC bimestriel	
Participants	OCS Security : - BSO	Orange Cloud for Business : - Cloud Avenue
Documents en entrée	Documents supports du comité	
Documents en sortie	Compte rendu	

Cette fréquence peut être ajustée par le Business Security Officer selon les besoins de Cloud Avenue.

3.2.3.2. Indicateurs et tableaux de bord

La SSI du Contrat sera pilotée au travers d'indicateurs qui seront tous produits par le BSO et analysés en détail lors du comité sécurité.

Ci-après, la liste des éléments applicables au contrat et leur fréquence de reporting.

3.2.3.2.1. Indicateurs Primaire (Run)

Security Weather and Reporting

01 — Bimestriel – SW01

Security Governance

La gouvernance Sécurité est une instance qui permet de suivre régulièrement l'avancement la sécurité de l'offre avec les opérationnels Global Platforms & Services. La gouvernance est animée par le Business Security Officer.

02 — Bimestriel – SW02

Security Committee

Présenté en comité de sécurité, le tableau de bord sécurité contient les différents indicateurs du présent Plan d'Assurance Sécurité et relate plus généralement l'état de santé de la solution Global Platforms & Services Cloud.

03 — Bimestriel – SW03

Security Incident Reports

Le Business Security Officer rapporte l'évolution du nombre d'incidents de sécurité avec impact sur l'offre. Il est fait mention du détail complet pour chaque incident de sécurité.

04 — Annuel – SW04

Security Assurance Plan Update

La revue et la mise à jour du Plan d'Assurance Sécurité en relation avec le client est effectuée sur une base périodique, annuelle par défaut. Les indicateurs sont également revus selon la nécessité.

05

Annuel – SW05

Security Risk Assessment Update

Une analyse de risque est conduite par le Business Security Officer à l'implémentation du projet. La revue en relation avec le client est effectuée sur une base périodique, annuelle par défaut.

04

Annuel – SW06

Privacy Risk Assessment Update

Une analyse sur la protection des données personnelles est conduite par le Business Security Officer. La revue en relation avec le client est effectuée sur une base périodique, annuelle par défaut.

Vulnerability Review

01

Mensuel – VR01

Vulnerabilities Management

Le Business Security Officer réalise une veille des vulnérabilités pouvant affecter les machines de la solution. Un rapport est formalisé sous forme d'indicateurs et rapporté en comité de sécurité.

02

Mensuel – VR02

Vulnerability Health

Une attention particulière est apportée aux vulnérabilités de niveau 4 (Haute) et 5 (Critique). Cet indicateur est revu en comité de sécurité. Un rapport est formalisé et rapporté en comité de sécurité.

Technical Review

01

Mensuel – TR01

Patch Management

Les services de « Patch Management » sont fournis par nos équipes opérationnelles et suivent le processus classique OCB. Ceci est un rappel que la sécurité est prise en compte dans toutes les phases du projet.

04

Mensuel – TR04

Business Continuity and Disaster Recovery Plan

Les tests de « BCP /DRP » sont fournis par nos équipes opérationnelles et suivent le processus classique OCB. Ceci est un rappel que la sécurité est prise en compte dans toutes les phases du projet

Security Awareness

01

Annuel – SA01

Specific Security Awareness (OCB Administrators)

Une sensibilisation à la sécurité globale, grand publique, est dispensée à tous les intervenants sur le périmètre du présent contrat

3.2.3.2.2. Indicateurs Complémentaires (Run)

Security Follow-Up

01

Sur Demande – SF01

Security Actions Plan

Le Business Security Officer propose et suit un plan d'actions d'améliorations de la sécurité. Un rapport/suivi est formalisé et rapporté en comité de sécurité.

02

Sur Demande – SF02

Data Security Measures

Une attention particulière est apportée aux vulnérabilités de niveau 4 (Haute) et 5 (Critique). Cet indicateur est revu en comité de sécurité. Un rapport est formalisé et rapporté en comité de sécurité.

Security Review

01

Trimestriel – SR01

Accounts Access Review

Le Business Security Officer fait une revue de l'ensemble des comptes de la plate-forme et valide les accès. Il rend compte en comité de sécurité.

02

Annuel – SR02

Password Policy Review

Le Business Security Officer vérifie la politique des mots de passe mis en place sur l'ensemble des comptes de l'offre. Il rend compte en comité de sécurité.

Annuel – SR03

03 Password Rotation Review

Le Business Security Officer vérifie que la politique des mots de passe, et notamment la vérification du changement régulier de ceux-ci sur l'ensemble de l'offre.

Technical Review

Mensuel – TR05

05 System Configuration Review

Le Business Security Officer suit l'évolution des configurations système pour identifier tous changement susceptible de baisser le niveau de sécurité et/ou identifier les opportunités de durcissement.

Mensuel – TR06

06 Operation System Obsolescence

Le Business Security Officer met en évidence et suit l'évolution de l'obsolescence des systèmes d'exploitation et applicatives qui composent le parc du contrat.

Bimestriel – TR07

07 Infrastructure Obsolescence

Le Business Security Officer met en évidence et suit l'évolution de l'obsolescence des équipements réseau, stockage et hyperviseurs qui composent le parc du contrat.

Mensuel – TR08

08 Specific Operating System Hardening

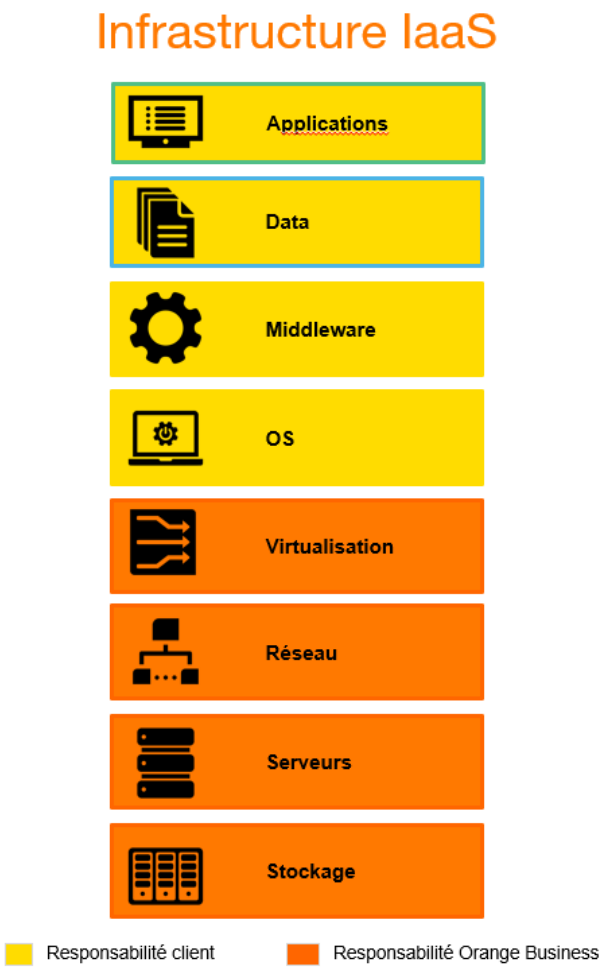
Additionnement au durcissement mis en place par OCB, le Business Security Officer prendra en compte les exigences de durcissement complémentaire du client.

Physical Security Review

Sur demande, le client peut demander à visiter nos centres d'hébergement afin de vérifier la bonne mise en œuvre des mesures décrites dans ce document.

3.2.3.3. RACI

Cloud Avenue étant une infrastructure de type IaaS (Infrastructure As A Service). Le modèle de responsabilité suivant est appliqué :



Sur la gestion de la sécurité, le modèle de responsabilité est le suivant :

Run (Primary)

Bundle	ID	Indicateurs	BSO	"Client"	OPS OCB
Security Weather and Reporting	SW01	Security Governance	R	A	C, I
	SW02	Security Committee	R	A	C, I
	SW03	Security Incident Reports	R	A	C, I
	SW04	Security Assurance Plan Update	R	A	C, I
	SW05	Security Risk Assessment Update	R	A	C, I
	SW06	Privacy Risk Assessment Update	C, I	A	R
Vulnerabilities Review	VR01	Vulnerabilities Management	A, R	C, I	R
	VR02	Vulnerability Health	A, R	C, I	R
Technical Review	TR01	Patch Management	C, I	A	R
	TR02	Application Management	C, I	A	R
	TR03	Antivirus Management	C, I	A	R
	TR04	Business Continuity and Disaster Recovery Plan	C, I	A	R
Security Awareness	SA01	Specific Security Awareness (OCB Administrators)	C, I	A	R

Run Options (Recurring / On Demand)

Bundle	ID	Indicateurs	BSO	"Client"	OPS OCB
Security Follow-Up	SF01	Security Actions Plan			
	SF02	Data Security Measures	R	A	C, I
Security Review	SR01	Accounts Access Review	R	A	C, I
	SR02	Password Policy Review	R	A	C, I
	SR03	Password Rotation Review	R	A	C, I
Technical Review	TR05	System Configuration Review	C, I	A	R
	TR06	Operation System Obsolescence	R	A	C, I
	TR07	Infrastructure Obsolescence	R	A	C, I
	TR08	Specific Operating System Hardening	C, I	A	R
	TR09	Traceability (LOG, SIEM Intégration)			
Physical Security (ZRR, PPST) Review	PS01	Physical Access Review			
	PS02	Access controls - Anti-intrusion Device			
	PS03	Human and Physical Security Device			
	PS04	Map Access Areas and Premises	C, I	A	R
Administration Bastion (CASA CyberArk) Review	CR01	Audit CyberArk Users Entitlement Rights	C, I	A	R
	CR02	Audit Logs Activities in the Safes.			
Security Awareness (Users/Adminstrators)	SA02	Global Security Awareness (All Users)			
	SA03	Specific Security Awareness (Developpers)			

3.3. Sécurité liée aux ressources humaines

Ce chapitre correspond à la thématique 7 de l'ISO 27002 version 2017.

3.3.1. Maîtrise des intervenants

Une liste des intervenants sur Cloud Avenue est maintenue à jour dans le cadre du processus de gestion des entrées/sorties. Cette liste est notamment utilisée comme référentiel pour effectuer la revue des habilitations logiques (cf. 3.5 - Contrôle d'accès). Les droits d'accès des intervenants sont modifiés/supprimés dès qu'ils changent de fonction ou qu'ils quittent la société.

3.3.2. Sélection des candidats

Les candidats sélectionnés à l'embauche sur la base de CV et lettre de motivation sont soumis à de multiples vérifications dans le respect de la réglementation locale de l'embauche comprenant sans s'y limiter à une vérification de la carte d'identité, la récupération des diplômes ou attestations de réussites (certifications, recommandations...).

Le contrôle des intervenants par les autorités s'effectue dans le cadre de la réglementation locale au lieu de l'embauche.

3.3.3. Sensibilisation

Des actions de sensibilisation à la sécurité des Systèmes d'Information ont principalement lieu au travers de formations dispensées à tout le personnel Orange.

Le suivi de formation est réalisé mensuellement avec des relances automatiques des personnes n'ayant pas été sensibilisées, et avec un questionnaire post-formation permettant de mesurer les acquis.

D'autres actions sont régulièrement menées pour maintenir le niveau de sensibilité au travers messages de communication sur les bonnes pratiques de sécurité, et d'intervention d'experts sécurité dans les réunions d'équipe. En cas de menace plus imminente, des messages d'alerte sécurité sont envoyées à l'intégralité du personnel (ex : campagne de phishing).

Des sensibilisations plus spécifiques aux risques sécurité sont réalisées semestriellement sur la population des top managers, notamment aux risques légaux et réglementaires.

Un espace est mis à disposition du personnel sur le réseau social de l'entreprise pour retrouver les supports de formation, des guides spécifiques, et pour pouvoir poser des questions aux experts sur le forum.

3.3.4. Engagement écrit des intervenants

Engagement de confidentialité des intervenants

Les salariés ont une obligation générale de discrétion inscrite dans leur contrat de travail et/ou dans leur convention collective. Ci-après un extrait d'un contrat de travail Orange :

« Article 10 : Secret professionnel et devoir de discrétion

Comme l'ensemble du personnel d'Orange, Madame/Monsieur _____ est tenu(e) au secret professionnel absolu. Cette prescription s'applique pendant l'exécution et la suspension du contrat de travail ainsi qu'après sa rupture et concerne notamment les techniques mises en œuvre par Orange, ainsi que toutes études et travaux exécutés dans l'entreprise.

Elle s'applique également à toute information ayant un caractère confidentiel, en particulier celles qui ne sont pas habituellement communiquées au public, que Madame/Monsieur _____ pourrait recueillir à l'occasion de ses fonctions ou du seul fait de sa présence à Orange.

Le non-respect de cette prescription de secret constituerait une faute et pourrait faire l'objet de poursuites civiles et/ou pénales. »

Pour les offres santé, les exploitants Orange signent un engagement de confidentialité renforcé, dont voici un extrait :

CLAUSE DE SECRET PROFESSIONNEL

<NOM PRENOM> s'engage à ne divulguer à quiconque les données de santé à caractère personnel auxquelles il a accès à partir de la plateforme d'hébergement de ces données de santé dans le cadre de ses fonctions au sein de l'entité Orange <ENTITE>, et reconnaît être soumis au secret professionnel concernant ces données conformément à l'article L.1111-8 du code de la santé publique.

<NOM PRENOM> est informé du fait que le non-respect de cette clause est sanctionné pénalement par l'article 226-13 du code pénal.

Cette obligation de secret professionnel se prolongera après la cessation du Contrat de travail, quelle qu'en soit la cause.

Pour les sous-traitants, cet engagement est signé par l'intervenant via son employeur (cf. partie 3.11).

Charte de bon usage des ressources informatiques

De même, tout salarié doit, de par le règlement intérieur, respecter la charte de bon usage des ressources informatiques.

3.4. Gestion des actifs

Ce chapitre correspond à la thématique 8 de l'ISO 27002 version 2017.

3.4.1. Inventaire des actifs

La liste des actifs supports (routeurs, commutateurs, pare-feux, baies de stockage, serveurs, machines virtuelles, logiciels…) des offres Cloud est maintenue dans des outils de cartographie internes Orange. Ces outils tracent à la fois les composants de l'infrastructure de Cloud Avenue et les composants des environnements clients (ex : Virtual Machine, pare-feux virtuels …).

Ces inventaires sont mis à jour dans le cadre du processus de gestion des changements.

3.4.2. Mesures de protection des actifs supports

Classification des ressources d'infrastructure

Les ressources d'infrastructures sont classifiées sur une échelle à 4 niveaux, définie dans la Global Security Policy d'Orange, et permettant de qualifier le préjudice pour Orange et ses clients en cas d'incident sur la ressource :

- **Niveau 4** : impact vital, enjeux très importants (voire vitaux) correspondant à des risques inadmissibles ;
- **Niveau 3** : impact critique, enjeux importants correspondant à des risques dont les effets doivent être limités ;
- **Niveau 2** : impact sensible, enjeux modérés et risques maîtrisés avec un tort limité pour l'entreprise ;
- **Niveau 1** : impact nul ou quasi-nul.

Toutes les ressources de Cloud Avenue hébergées dans nos datacenters (routeurs, commutateurs, baies de stockage et de sauvegarde, serveurs, …) sont considérées au minimum de **niveau 3** (soit niveau 3 ou niveau 4). Les mesures associées à la protection de ces ressources critiques sont décrites tout au long de ce document.

Classification, marquage et protection de la documentation

La documentation est classifiée puis marquée, conformément aux règles internes Orange définies dans le document « Marquage des documents ». Cinq niveaux y sont définis : **diffusion libre**, **interne Orange**, confidentiel Orange et **secret Orange.**

Les documents opérationnels des projets / offres Cloud Avenue sont stockés sur des serveurs de fichier. L'accès est protégé par un contrôle d'accès nominatif et une gestion des droits gérée selon le principe du besoin d'en connaître.

Classification des informations clientes

La classification des informations clientes hébergées sur l'offre Cloud Avenue est sous la responsabilité des clients.

3.4.3. Effacement des données

Protection des données clientes désallouées

Les données clientes situées sur des ressources désallouées ne peuvent pas être accédées par un autre client. Cette protection est assurée par les mécanismes internes propres aux produits utilisés par Orange. Par exemple, les produits VMWARE assurent qu'en cas de réallocation de ressources de stockage, le nouveau client ne peut pas lire les données de l'ancien client.

Suppression des données clientes en fin de contrat

En fin de contrat, l'ensemble des ressources affectées aux clients sont désallouées, et les données clientes deviennent inexploitables, comme évoqué dans le paragraphe précédent.

Seules les sauvegardes sont conservées quelques mois par Orange après la fin de contrat (délai spécifique à chaque offre – généralement de l'ordre de 3 mois). Passé ce délai, Orange ne détient plus aucune donnée du client.

3.5. Contrôle d'accès

Ce chapitre correspond à la thématique 9 de l'ISO 27002 version 2017.

Orange assure le contrôle d'accès sur les environnements qui sont contractuellement sous sa responsabilité. Le contrôle d'accès sur les systèmes et applications managés par le client sont sous la responsabilité du client.

3.5.1. Contrôle d'accès pour les exploitants d'Orange

Moyens d'accès

Les exploitants d'Orange administrent l'infrastructure Cloud Avenue (serveurs, baies de stockage, équipements réseaux, équipements de sécurité…) de la manière suivante :

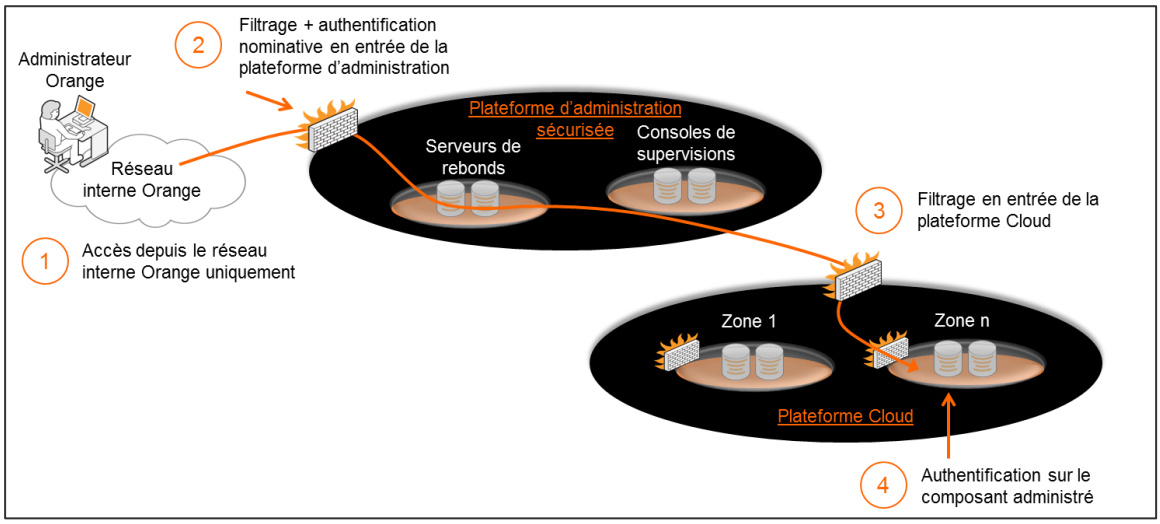
Remarque : pour certaines offres, les VM clientes peuvent être managées par Orange, on parle alors d'offre managées ou co-managées. Ce mode d'administration spécifique n'est pas décrit dans ce paragraphe mais dans les spécificités de chaque offre (qui font l'objet de white paper spécifique à ces offres).

- 1 – Accès depuis le réseau interne Orange. L'administration de l'infrastructure Cloud n'est possible que depuis le réseau interne Orange.
- 2 – Filtrage et authentification nominative en entrée de la plateforme d'administration. La plateforme Cloud Avenue est protégée du réseau interne Orange par une zone de sécurité intermédiaire, appelée plateforme d'administration, laquelle héberge des serveurs de rebonds. Cette étape permet d'assurer :
  - Du filtrage réseau ;
  - De l'authentification nominative et du traçage des accès ;
  - De la journalisation des sessions sur un serveur de log centralisé ;

- De l'autorisation : l'administrateur ne peut accéder qu'aux ressources autorisées pour son profil.

- 3 – Filtrage sur la plateforme Cloud. Ce nouveau niveau de filtrage permet de s'assurer que les flux d'administration de l'infrastructure Cloud proviennent exclusivement de la plateforme d'administration.
- 4 - Authentification des exploitants sur les environnements Cloud. L'administrateur habilité s'authentifie sur le composant qu'il souhaite administrer :
  - Authentification avec des comptes centralisés (AD, TACACS+) ou locaux ;
  - Journalisation des sessions sur un serveur de log centralisé ;
  - Autorisation : l'administrateur ne peut accéder qu'aux ressources autorisées par son profil.
  - Traçabilité : traçage des actions administrateurs, renouvellement automatique des mots de passe des serveurs.

Les accès d'administration sont toujours réalisés de manière sécurisée via le protocole SSL/TLS (exemples de flux : HTTPS, SSH).



Authentification et gestion des mots de passe

Les connexions avec les comptes d'exploitation respectent la politique interne de gestion de mot de passe (*référence « PLS-GS001 - Password Security Policy.pdf », document confidentiel, mais consultable partiellement dans les locaux d'Orange après signature d'un engagement de confidentialité*) :

- Complexité
  - Le mot de passe doit être au minimum composé de 8 caractères. Il est recommandé d'utiliser 14 caractères ;
  - Le mot de passe doit être composé au minimum d'une majuscule, d'une minuscule, d'un caractère numérique et d'un caractère spécial ;
  - Le mot de passe ne doit pas être composé d'une sous-chaîne contenant le nom, prénom, identifiant commercial, société ;
  - Les mots de passe par défaut des constructeurs/éditeurs doivent être modifiés dès la phase d'installation.
- Renouvellement

    - Le mot de passe doit être renouvelé à minima tous les 6 mois ;
    - Le mot de passe doit être différent des 2 derniers mots de passe utilisés. Il ne doit pas être modifié trop fréquemment (ex : 15 jours).
- Verrouillage
    - Le compte doit être verrouillé automatiquement après 5 tentatives d'authentification infructueuses ;
    - Le compte doit être verrouillé automatiquement si la date d'expiration du mot de passe est dépassée.
- Protection du mot de passe
    - Les mires d'authentification doivent être accessibles uniquement par des communications chiffrées et sécurisées ;
    - Le mot de passe saisi ne doit pas s'afficher en clair ;
    - Le mot de passe ne doit pas être stocké en clair (ex : seule son empreinte (hash) doit l'être).
- Durée de session
    - Les sessions inactives doivent être fermées automatiquement après une durée déterminée pour chaque offre.
- Journalisation
    - Les événements liés à l'authentification doivent être notifiés dans un fichier journal.

Pour les personnels, un token disposant d'un certificat est fourni par le système de PKI (public key infrastructure) du groupe Orange est stocké sur ce token pour assurer une authentification forte supplémentaire.

Procédure d'attribution et de révocation des droits pour les exploitants d'Orange

La procédure d'attribution/révocation d'un compte et des droits associés, appelée CARM (Controlling Access Rights Management) est appliquée et contrôlée. Cette procédure est une mesure de sécurité du SMSI (Systèmes de Management de la Sécurité de l'Information) certifié ISO 27001, mis en place par Orange.

Les comptes partagés ne sont autorisés que de manière exceptionnelle sous forme de dérogation. Ils doivent être listés et justifiés.

Revue des droits pour les exploitants d'Orange

Une revue des habilitations et des droits est effectuée tous les trimestres. L'activité consiste à extraire la liste des personnes ayant un compte opérationnel sur Cloud Avenue. Cette liste est recoupée par manager qui va définir si le compte doit être maintenu ou non. Si le compte opérationnel n'est pas plus nécessaire il est alors supprimé.

En cas de découverte de droits illégitimes, les mesures adéquates sont appliquées :

- Suspension du compte ;
- Examen des traces d'utilisation pour révéler d'éventuels incidents ;
- Prise de mesures correctrices (mise à jour des procédures, sensibilisation du management…).

Ces revues font l'objet d'un compte-rendu.

3.5.2. Contrôle d'accès pour les clients d'Orange

Les clients se connectent aux environnements Cloud Avenue à des fins d'administration ou d'accès aux services applicatifs. Les accès sont réalisés via Internet et/ou un réseau privé (VPN client) en fonction des offres et des options sélectionnées par le client.

Les accès clients sont toujours réalisés de manière sécurisée via le protocole SSL/TLS (exemples de flux : HTTPS, SSH) :

- L'authentification serveur (portails d'administration, serveurs applicatifs) est systématiquement réalisée via un certificat X.509 « serveur » délivré par une autorité de certification reconnue.
- L'authentification client est réalisée sur la base d'un login/mot de passe transmis préalablement de manière sécurisée à chaque client. Pour certaines offres, il est possible de mettre en œuvre une authentification forte (usage de token logiciel générant un mot de passe à usage unique, usage de certificat X.509 « client »).
- Les flux réseaux sont systématiquement chiffrés selon l'état de l'art.

Le client porte la responsabilité de la sécurité des éléments d'authentification qui lui sont communiqués par Orange. Dans la mesure des possibilités offertes par les outils, Orange impose une complexité minimale sur tous les mots de passe manipulés par le client.

Pour certaines offres, le client a la possibilité de créer lui-même des comptes d'accès (profils utilisateur, administrateur). Les identifiants et les droits d'accès associés sont sous la responsabilité du client.

L'ensemble des connexions client est tracée dans des journaux d'événements (Logs) qui sont archivés conformément à la législation en vigueur. Pour certaines offres, le client a la possibilité d'accéder aux Logs dont il porte la responsabilité légale.

3.6. Cryptographie

Ce chapitre correspond à la thématique 10 de l'ISO 27002 version 2017.

Suites cryptographiques - Toutes les suites cryptographiques utilisées sur les offres Cloud Avenue (ex : AES 256, SHA-256, TLS 1.2) sont basées sur les standards du marché dont le niveau de sécurité est éprouvé. L'étude technique de l'ENISA[6], « Algorithms, Key Size and Parameters Report, 2013 Recommendations » a en particulier été prise en compte pour choisir les suites cryptographiques. Les flux d'administration sont systématiquement chiffrés en utilisant le protocole SSL/TLS.

Gestion des certificats – Les certificats d'authentification des serveurs se basent sur des autorités de certifications (ex : VeriSign, Thawte…) reconnues par les principaux navigateurs

[6] ENISA : European Network and Information Systems Agency

Web. Les certificats d'authentification pour nos services d'administration internes (accessibles uniquement par les exploitants Orange) peuvent se baser sur des certificats X.509 générés par l'autorité PKI de certification interne d'Orange.

Chiffrement des disques durs des exploitants Orange – Pour la sécurisation des données sensibles, les exploitants Orange disposent d'une solution de chiffrement supplémentaire avec authentification par token (ZoneCentral de Prim'X). Cette solution a été certifiée EAL3+ sur sa version 3.1 par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

3.7. Sécurité physique et environnementale

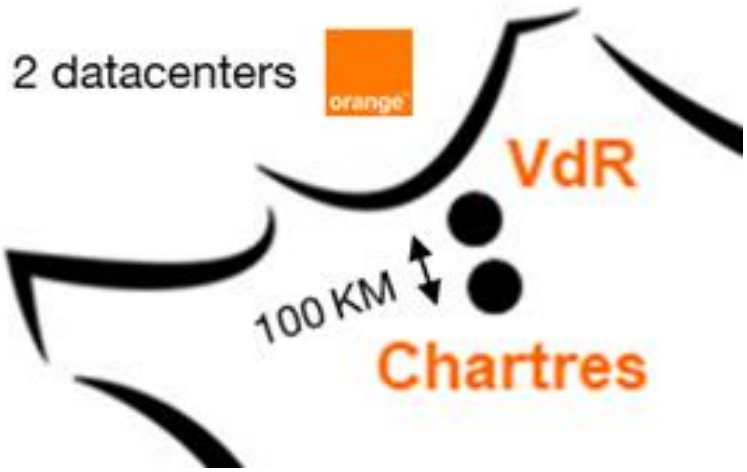
Ce chapitre correspond à la thématique 11 de l'ISO 27002 version 2017.

La sécurité physique et environnementale vise à protéger le système d'information d'Orange et de ses clients contre :

- Les menaces environnementales et les sinistres : explosion, séisme, incendie, dégât des eaux, panne électrique, panne de la climatisation, panne télécoms…
- Les menaces d'intrusions physiques : accès en salle d'une personne non habilitée, vol de disques durs contenant des informations sensibles…

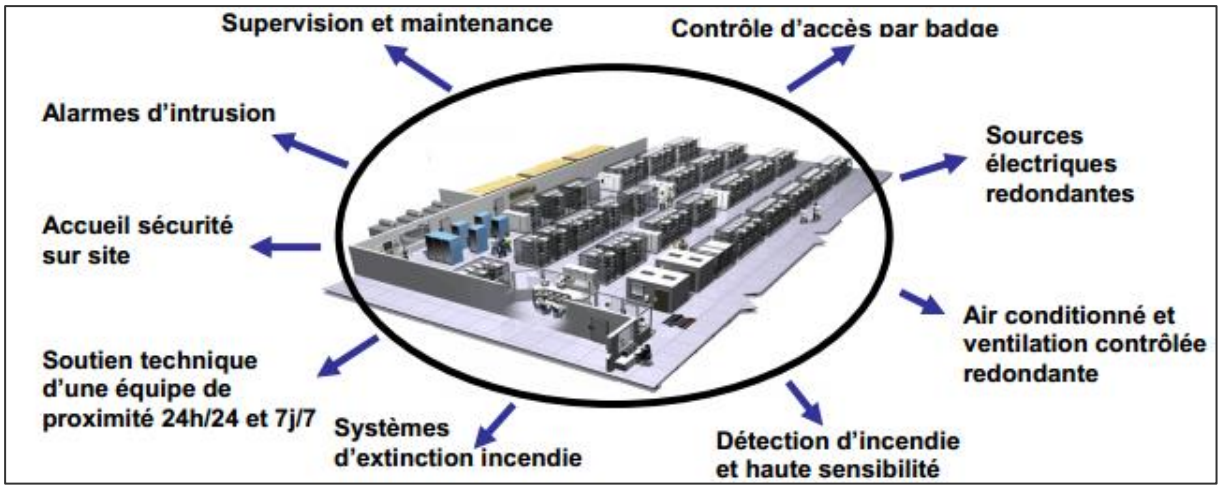
Sécurité physique et environnementale de nos centres d'hébergement

Notre offre Cloud Avenue (infrastructures, sauvegardes…) est hébergée sur plusieurs centres d'hébergement (« datacenters »). Les sites d'hébergement de Cloud Avenue sont Val-De-Reuil et Chartres. Le site de principal est celui de Val-De-Reuil, Chartres est le site de backup



Localisation des 2 Datacenters sur Cloud Avenue

Les mesures de sécurité suivantes sont mises en œuvre au niveau de ces centres d'hébergement d'Orange :



ISAE 3402 - Tous les centres d'hébergement mentionnés ci-dessus sont certifiés ISAE 3402 Type II (ex SAS 70). ISAE 3402 est le standard permettant aux clients qui externalisent d'obtenir une assurance quant à la fiabilité du dispositif de contrôle interne de leurs prestations de service. Depuis le 15 juin 2011, il se substitue au standard SAS 70 et est applicable aux engagements internationaux. À ce titre, des auditeurs indépendants se sont livrés à des contrôles rigoureux au cours d'une période de test de 12 mois pour valider la qualité, la fiabilité et l'intégrité des processus et contrôles opérationnels d'Orange. Ce rapport d'audit indépendant assure aux clients d'Orange Business que les services dont ils bénéficient répondent aux exigences de la loi Sarbanes-Oxley aux États-Unis et respectent des **objectifs clés de sécurité**, de gestion du changement et de continuité des services.

Classification TIER[7] - Les datacenters de l'offre Cloud Avenue sont construits et opérés pour satisfaire aux exigences TIER IV (cf. définition en annexe A).

Comme précisé en annexe A, le niveau TIER IV est le niveau le plus performant de la classification TIER.

Tolérance aux pannes et à la maintenance - Les architectures techniques mises en œuvre permettent de répondre aux contraintes d'exploitation suivantes :

- Absence d'impact sur la charge lors du premier défaut.
- Grande tolérance aux pannes, jusqu'à 2 défauts majeurs sans impact.
- Absence d'interruption de service lors d'une intervention de maintenance.

Le mode de gestion et les processus mis en œuvre permettent d'assurer la sécurité des personnes, des bâtiments et des équipements hébergés.

[7] TIER : cf. définition en annexe 4

L'architecture mise en place pour Cloud Avenue comprend la répartition sur les 2 sites (Val-De-Reuil et Chartres) en mode actif/actif au niveau serveur. L'accès Internet pour sa part doublé en mode actif/passif sur les 2 sites.

Spécifications détaillées dans les livrets de site[8] - Les spécifications de nos centres d'hébergement sont détaillées dans des livrets de site qui abordent les thématiques suivantes :

- Energie (redondance des adductions, redondance des tableaux généraux de distribution de la basse tension, groupe électrogène d'une autonomie minimale de 72 heures, onduleurs …) ;
- Climatisation (redondance N+1, c'est-à-dire que la panne d'une climatisation n'a aucun impact sur la chaîne de production de froid) ;
- Urbanisation (allées, faux-planchers …) ;
- Protection incendie (détection, extinction, centrale de supervision, …) ;
- Protection dégâts des eaux (détection, pompes …) ;
- Protection contre les intrusions (barrières/murs de sécurité, contrôle d'accès, vidéo-surveillance, gardiens, rondes, détection d'intrusion, gestion des invités …) ;
- Organisation de la sécurité sur les sites (responsables, surveillance 24/7, réactivité, …) ;
- Sécurité de l'environnement (absence de risque naturel …).

Sécurité physique et environnementale de nos plateaux d'exploitation

Les plateaux d'exploitation sont les locaux depuis lesquels sont exploitées par Orange les offres Cloud Avenue. Les différents plateaux sont :

- MSC Inde et Egypte : support niveau 1 et niveau 2 des infrastructures motorisant les offres Cloud (firewall, serveurs, réseau…) ;
- Site Orange/France : support niveau 2 sur certaines offres spécifiques et support niveau 3 de Cloud Avenue.

Les plateaux d'exploitation suivants disposent d'une certification sécurité ISO 27001 délivrée par l'AFNOR : site de Cesson-Sévigné, d'Inde et d'Egypte. Le périmètre fonctionnel de la certification est la mise en œuvre, la fourniture et le support de services infogérés et de solutions de communication.

Dans le cadre de la fourniture des services cloud, Orange Business peut avoir à transférer des données du client en dehors de l'Union Européenne vers les MSCs mentionnés ci-dessus. Au sein d'Orange Business, un "Agreement for the transfer of customer personal data" est en vigueur depuis le 2 janvier 2013. Selon cet « Agreement », les données personnelles que les clients (en tant que responsables de traitement) transfèrent à Orange Business (en tant que sous-traitant ou sous-traitant ultérieur) bénéficient d'un niveau de protection adéquat tel qu'exigé par la Commission Européenne. Chaque entité légale d'Orange Business située en dehors de l'Union Européenne dans un pays n'assurant pas un niveau de protection adéquat tel qu'exigé par la Commission Européenne, s'est engagée, en

[8] Livrets de site : ces livrets sont confidentiels, mais consultables dans les locaux d'Orange après signature d'un engagement de confidentialité.

signant cet « Agreement », à respecter la Directive Européenne 95/46/EC, et a ainsi accepté d'être liée par les clauses standards de la Commission Européenne.

3.8. Sécurité opérationnelle

Ce chapitre correspond à la thématique 12 de l'ISO 27002 version 2017.

3.8.1. Gestion des procédures opérationnelles

Certification ISO 20000 et ITIL

La gestion des services par Orange Business est certifiée ISO 20000[9]. Les exigences de la certification ISO 20000 sont alignées avec les meilleures pratiques de la dernière version d'ITIL (v3 2011) pour les processus tels que la fourniture des services, la gestion des relations, la résolution de problèmes, le contrôle et la mise en production, les exigences de sécurité renforcées.

Gestion des changements

La gestion des changements est réalisée selon le modèle ITILv3 ; cela concerne notamment les changements relatifs à la sécurité. La gestion des changements est opérée sous la responsabilité d'un « change manager ».

- Les changements « standards », c'est-à-dire pré-identifiés dans un catalogue, suivent un processus simplifié, et ne nécessitent pas une étude préalable par un expert sécurité.
- Les changements identifiés comme étant "non-standard" (évolutions) sont formalisés dans des RFC (Request For Change) avec un passage en réunion CAB (Change Advisory Board). Les RFC font l'objet d'une étude sécurité préalable par un expert sécurité du « Centre de Compétence Sécurité Cloud » qui donne son avis sur celle-ci. La sécurité est donc représentée au CAB ; elle a autorité pour interdire un changement jugé dangereux ou non conforme à la politique de sécurité, et elle peut le faire en toute indépendance.

  Les CAB ont lieu régulièrement (à minima une fois par mois). Pour des changements à caractère urgent (exemple : mise à jour de sécurité critique), il est possible de traiter immédiatement la demande de changement dans le cadre d'une réunion ECAB (Emergency Change Advisory Board).

La gestion des changements mis en œuvre par Orange permet ainsi de :

- Minimiser l'impact des changements sur les services opérationnels et les utilisateurs ;
- Disposer de méthodes standardisées, procédures et mécanismes de contrôle ;
- Identifier les interlocuteurs habilités à demander un changement ;

[9] Certificat associé : https://certificats-attestations.afnor.org/certification=335171233155

- Contrôler les changements afin qu'ils correspondent à la politique de sécurité ;
- Formaliser l'évaluation correcte de l'impact, la priorité, les avantages et le risque d'un changement ;
- Définir des catégories de changements et de temps d'implémentation associés ;
- Gérer les priorités des changements en fonction des risques et impacts ;
- Améliorer la qualité de l'information et de la communication :
    - Assurer que toutes les parties concernées ont été impliquées pour limiter les incidents liés aux changements ;
    - Alimenter la base de données de configuration en informations correctes ;
    - Faire en sorte que tous les changements soient documentés ;
    - Communiquer pro-activement les indisponibilités planifiées aux utilisateurs/clients.

Gestion des capacités

La gestion des capacités est réalisée selon le modèle ITILv3 sous la responsabilité d'un « capacity manager ». L'objectif est d'assurer un niveau de service constant pour les clients. La gestion des capacités permet d'anticiper les futurs besoins des clients en analysant les mesures et les tendances de consommations sur les ressources composant l'infrastructure Cloud.

La gestion des capacités surveille et agit principalement sur :

- Les ressources CPU/RAM ;
- Les ressources réseaux (bande passante, espace d'adressage) ;
- Les ressources stockage et sauvegarde ;
- Les licences logicielles.

Pour Cloud Avenue, le « capacity manager » établit régulièrement des statistiques avec différents indicateurs propres à chaque offre (mesures techniques, prévisions commerciales).

3.8.2. Protection contre les codes malveillants

Environnement client

L'offre Cloud Avenue inclue un service antivirus dédié pour les environnements client. Ce service est restreint aux systèmes Microsoft Windows car le ratio risques / bénéfices n'a pas été jugés favorables pour les systèmes Linux.

L'agent antivirus installé sur les systèmes Windows met à jour sa base de signature virale régulièrement (à minima une fois par jour) auprès d'un serveur de mise à jour spécifique situé dans une zone de sécurité dédiée aux mises à jour des machines des clients. Ce serveur de base de signature antivirus est lui-même mis à jour en temps-réel sur des serveurs publics mis à disposition sur internet par l'éditeur de la solution antivirus.

3.8.3. Gestion des sauvegardes

Environnement client

Les données des environnements clients sont sauvegardées selon une politique de sauvegarde propre à chaque offre et en fonction des options sélectionnées par le client. De manière générale, les données clients sont sauvegardées automatiquement et de manière périodique avec une durée rétention qui dépend des offres.

Les sauvegardes peuvent être de différentes natures en fonctions des offres et des options. Exemple :

- Sauvegarde en mode fichier (« file level »), notamment pour les données applicatives ;
- Sauvegarde en mode image (« image level ») pour les machines virtuelles ;
- Sauvegarde de données brutes (serveur de fichiers).

Les modalités de restauration varient selon les offres :

- Restauration réalisée par le client de manière autonome ;
- Restauration réalisée par Orange sur demande de changement via le portail d'administration.

Pour l'offre Health Data Solutions, la politique de sauvegarde applicable est détaillée dans le Dossier de Spécification Détaillé.

Infrastructure Orange

Toutes les configurations des équipements des infrastructures Cloud Avenue sont sauvegardées régulièrement. Cela concerne notamment :

- Les serveurs : Windows, Linux, données applicatives (notamment les bases de données) ;
- Les équipements réseau (routeurs, switchs) ;
- Les équipements de sécurité (UTM firewall, Appliance VPN) ;
- Les équipements de stockage.

Pour les configurations statiques, les sauvegardes sont réalisées à chaque évolution de configuration. L'opération de sauvegarde est encadrée par le processus de gestion des changements.

Pour les configurations dynamiques, des agents réalisent des sauvegardes automatiques de manière périodique. La rétention des données de configuration est à minima de 14 jours (plusieurs versions de sauvegardes sont conservées).

Toutes les sauvegardes de configuration sont stockées sur des sites tiers (datacenter distinct) afin de garantir la disponibilité des données de configuration en cas de sinistre majeur sur le site de production. Pour les nouveaux datacenters, les sauvegardes de configuration sont réalisées sur le même site de production mais dans des salles informatiques différentes. Les sauvegardes sont stockées de manière sécurisée (cloisonnement logique) en fonction du besoin d'en connaitre.

3.8.4. Journalisation et supervision sécurité

Orange assure une supervision systématique de ses infrastructures et services Cloud, notamment d'un point de vue sécurité. Une journalisation des évènements (logs) est mise en œuvre sur l'ensemble des composants, notamment les composants sécurité. Cette journalisation a plusieurs objectifs :

- Détecter et analyser les incidents de sécurité ;
- Répondre aux obligations légales ;
- Permettre le Troubleshooting.

Tous les composants sont supervisés en 24/7 et des astreintes sont mises en place pour intervenir sur des incidents critiques, notamment lorsque la sécurité est impactée.

Nature des logs sécurité

Les évènements journalisés sont définis composant par composant, selon deux critères :

- Les exigences légales : En France, la LCEN[10] et CPCE[11].
- Les exigences de sécurité :
  - Évènements liés aux activités d'administration pour l'ensemble des composants ;
  - Évènements des composants de sécurité (exemple : les logs firewall).

En France, la journalisation et la supervision des journaux sont réalisées en respectant la Loi Informatique et Libertés.

---

[10] LCEN : Loi pour la Confiance dans l'Economie Numérique
[11] CPCE : Code des Postes et des Communications Electroniques

Centralisation des logs sécurité

Tous les composants des infrastructures Cloud remontent leurs logs périodiquement ou en temps réel sur des serveurs de collecte situés dans des zones de sécurité spécifiques. Les logs sécurité sont protégés en intégrité et uniquement accessibles par les administrateurs en charge de la sécurité. La rétention des logs est de 3 mois par défaut (troubleshooting et sécurité) et d'un an pour les logs légaux.

Surveillance pro-active des Logs de sécurité – Les serveurs de collecte des logs sécurité permettent une supervision humaine des évènements de sécurité selon des processus définis durant la phase de conception. Par exemple, l'absence de remontée de logs, l'augmentation soudaine du nombre d'événements ou le fait qu'un évènement précis se produise peuvent faire l'objet d'une analyse et d'un traitement. Cette supervision peut être proposée en option aux clients.

Référence unique de temps

L'horodatage des logs, notamment les logs sécurité, est réalisé avec une référence de temps unique pour tous les composants de Cloud Avenue. Le service de temps est fourni par différents serveurs NTP installés dans des zones de sécurité spécifiques. La référence de temps est fournie par un serveur physique dédié (serveur racine avec antenne GPS) installé dans les zones de services internes d'Orange Business.

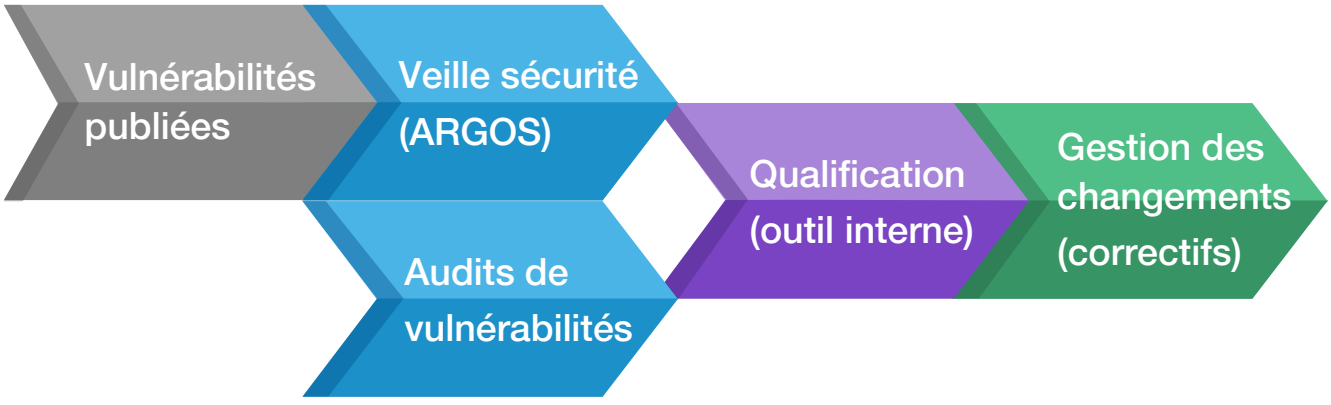
Consultation des Logs par le client

Dans Cloud Avenue, le client a la possibilité d'accéder aux Logs de son environnement, notamment les Logs des applicatifs et firewalls. Les accès aux Logs sont sécurisés et restreints à chaque environnement client.

3.8.5. Gestion des vulnérabilités techniques

La gestion des vulnérabilités a pour principal objectif le maintien en condition de sécurité des infrastructures et des services de Cloud Avenue. Les vulnérabilités sont identifiées dans le cadre d'une veille sécurité et de scans de vulnérabilités. Elles sont ensuite qualifiées avec un correctif à déployer en production.

La veille sécurité, le suivi du déploiement des correctifs et le reporting sont la responsabilité des « Responsables Sécurité Opérations ».



Veille sécurité

L'ensemble des composants fait l'objet d'une veille sécurité permanente qui a pour but d'identifier les vulnérabilités techniques pouvant impacter la sécurité des infrastructures et des services de Cloud Avenue.

La veille sécurité est alimentée par différents canaux :

- Les bulletins sécurité des éditeurs de produits (hyperviseur de virtualisation, équipements réseau et sécurité, OS…) ;
- Les rapports de veille : ARGOS, CVE, NIST NVD, CERT-FR … ;
- Les remontées des clients ;
- Les remontées de nos audits et de nos scans de vulnérabilités.

ARGOS est l'outil de veille sécurité du groupe Orange. Il permet aussi d'inventorier les différents produits (versions matérielles et logicielles) utilisés au sein de chaque offre en se basant sur la CMDB. Ainsi, les « Responsables Sécurité Opérations » des différentes offres sont alertés dès qu'une vulnérabilité est susceptible d'impacter les services dont ils portent la responsabilité.

Audits de Vulnérabilités

Des audits réguliers (ou permanents sur les infrastructures les plus critiques) sont lancés sur nos plateformes de production pour à la fois mesurer l'état des vulnérabilités de nos plateformes et potentiellement identifier des vulnérabilités n'ayant pas été analysées par la veille. Pour cela, Orange utilise des solutions de tiers leaders sur le marché des scans de vulnérabilités (Qualys).

Qualification des vulnérabilités

La qualification des vulnérabilités et des correctifs de sécurité est réalisée avec l'outil interne Orange « Vulnerability Management Tool (VMT) » sous la responsabilité conjointe de l'ingénierie d'Orange et de la direction de la sécurité. La qualification permet de statuer sur l'attitude à adopter : aucune action par exemple en cas de faille non-exploitable, changement de configuration, installation d'un patch de sécurité, identification d'un contournement.

Application des correctifs de sécurité

Tous les correctifs de sécurité qualifiés (évolution de configuration, patch de sécurité) sont déployés dans le cadre du processus de mise en production (gestion des changements) :

- Les vulnérabilités de niveau de criticité faible/moyen sont gérées dans le cadre des mises en production mineures ou majeures (CAB). Le planning est adapté aux contraintes opérationnelles d'Orange Business et aux engagements contractuels avec le client (créneau de maintenance…)
- Les vulnérabilités de niveau de criticité fort/critique sont gérées dans le cadre des mises en production urgentes (ECAB).

Les fichiers d'inventaire des équipements sont mis à jour suite à l'application des correctifs.

Reporting

Le Responsable Sécurité Opérations effectue un reporting mensuel interne de la veille sécurité et des vulnérabilités traitées sur la période. Ce reporting est réalisé via l'outil VMT d'Orange et n'est pas transmis aux clients pour des raisons de confidentialité.

En cas de vulnérabilité critique et susceptible d'impacter fortement ses clients, Orange Business peut communiquer directement avec ses clients à des fins d'information.

3.8.6. Sécurité des postes d'administration au sein d'Orange

Tous les postes des exploitants Orange utilisés pour administrer les infrastructures et services Cloud Avenue sont basés sur des modèles de configurations génériques et sécurisés :

- La configuration des postes (système d'exploitation, middleware et applications, droits utilisateurs) est durcie d'un point de vue sécurité. (master « E-buro » sur base OS Microsoft Windows) ;
- Présence systématique d'un antivirus mis à jour automatiquement et régulièrement ;
- Politique de mise à jour système avec des correctifs validés en interne Orange avant diffusion.

Les postes nomades et fixes intègrent l'outil de chiffrement de disque dur. De plus l'outil ZoneCentral est utilisé de manière complémentaire pour chiffrer des fichiers et répertoires sensibles. Zone Central est un produit de sécurité permettant le chiffrement des données contenues sur les disques durs des postes de travail pour en réserver l'accès aux seuls utilisateurs autorisés et identifiés. Il est directement interfacé avec le système PKI d'Orange, mais peut également être utilisé avec des utilisateurs externes via l'utilisation de conteneurs zed. L'utilisation de conteneurs zed est très largement utilisée pour assurer la communication sécurisée entre Orange et ses clients. Les outils ZoneCentral et zed ont fait l'objet d'une certification EAL3+ par l'ANSSI (ANSSI-CC-2012/07, et ANSSI-CC- 2016/25).

3.8.7. Politique de gestion des appareils mobiles

Pour les offres managées, les administrateurs opérationnels pourront se connecter à distance sur les différents environnements de Cloud Avenue depuis un poste d'administration sécurisé de type « e-buro » (voir §3.8.6).

La connexion au réseau d'administration (protégé par une gateway SSL/TLS et une authentification forte) depuis les appareils mobiles ne peut se faire que depuis le réseau interne Orange, accessible à distance via une liaison VPN IPSEC « Business Everywhere » filtrant les matériels et mettant en œuvre une vérification antivirale (sur poste et messagerie).

Une authentification à deux facteurs basée sur token matériel PKI est imposée pour les prestations de management sur Cloud Avenue.

3.9. Sécurité des communications

Ce chapitre correspond à la thématique 13 de l'ISO 27002 version 2017.

3.9.1. Sécurité des architectures Cloud Orange

Principes généraux

Les architectures des différentes zones de Cloud Avenue sont validées par un responsable sécurité Ingénierie placé sous la gouvernance du Chief Security, Risk and Compliance Officer. Ce dernier est garant de la cohérence des différentes architectures d'un point de vue sécurité.

Cette démarche basée sur un modèle prédéfini d'architecture offre plusieurs avantages :

- Simplification de la mise en œuvre d'une nouvelle offre Cloud ;
- Homogénéité des pratiques et des architectures entre les différentes offres ;
- Mutualisation de certains équipements ;
- Garantie sur la sécurité des offres : les modèles sont validés puis leur mise en œuvre est contrôlée par le Centre de Compétence Sécurité Cloud. Le niveau de sécurité de chaque nouvelle offre est également évalué par des audits et des tests d'intrusions avant toute mise en production. Il en est de même pour toute évolution majeure. Les résultats des audits et des tests d'intrusions internes ne sont pas diffusés aux clients pour des raisons de confidentialité ;
- Simplification du maintien en condition de sécurité.

Une analyse de risque systématique à chaque nouvelle offre complète la validation sécurité de l'architecture. Ces 2 actions constituent les bases de la démarche « SecurityInTTM » garantissant la prise en compte de la sécurité dans le design des offres.

Domaines de confiance et Zones de sécurité

L'architecture de Cloud Avenue applique le même modèle consistant à séparer les domaines de confiances, notamment le Back-end (interne Orange) et le Front End qui supporte les services Cloud exposés aux clients. Le cloisonnement back-end/front-end est physique, c'est-à-dire que des serveurs sont dédiés au back-end et d'autres dédiés au front-end.

Au sein de chaque domaine de confiance, des zones de sécurité assurent un cloisonnement logique par la mise en œuvre de certaines fonctionnalités telles que :

- La virtualisation (machines virtuelles, firewall virtuels, Load-balancer virtuels, routeurs virtuels/VRF) ;
- Les VLAN (802.1Q) ;
- Les réseaux virtuels VPN (IPSec, SSL) ;
- Le stockage virtuel (disques virtuels).

Ce cloisonnement logique garantit notamment l'isolation des différents environnements client.

Les communications (flux réseau) entre les différentes zones de sécurité sont systématiquement contrôlées par des firewalls (filtrage de type stateful). La configuration locale des différents composants est également réalisée de manière à renforcer le cloisonnement et la sécurité (exemple : ACL dans les routeurs).

Infrastructure Orange

Les serveurs d'infrastructure sont regroupés par zones de sécurité selon leur fonction (serveur d'administration, serveur frontal utilisé par les clients), leur nature (base de données, serveurs web) et leur niveau d'exposition (par exemple accessible ou non par les clients). Ainsi, des zones de sécurité sont dédiées aux outils d'exploitation d'Orange.

De manière générale, tous les serveurs disposent d'une interface dédiée aux flux de données et d'une interface technique dédiée aux flux de service (administration notamment).

Tous les composants des infrastructures cloud (serveurs, firewall, routeurs, baies de stockage…) sont configurés sur la base de guides de configuration sécurisés (guidelines) établis par les différentes ingénieries avec le concours d'experts sécurité du groupe Orange.

Environnements clients

L'isolation entre les environnements clients est basée sur les fonctions de virtualisation décrites précédemment. Au sein de Cloud Avenue, le client a la possibilité de gérer des fonctions de sécurité (firewall virtuel notamment). Les fonctions fournies aux clients varient selon les offres et les options sélectionnées.

Plus de détails sur cette solution peuvent être trouvé à ce lien.

3.9.2. Sécurité des échanges

Sécurité des flux internes Orange

Les moyens suivants sont mis en place pour sécuriser les échanges internes Orange :

- Réseaux : Les réseaux d'interconnexion entre les plateformes Cloud et les plateaux d'exploitation sont protégés par une ou plusieurs des solutions suivantes :
  - VPN MPLS ;
  - Tunnels chiffrés (IPSec, TLS) ;
  - Réseau de fibres dédié.
- Messagerie : A la demande des clients, les échanges de données sensibles effectués par mail entre les clients et Orange Business peuvent être chiffrés par un outil tiers convenu avec le client (ex : Orange recommande zed).
- Flux d'administration : Les flux d'administration sont protégés conformément à l'état de l'art avec des connexions de type SSL/TLS (SSH, HTTPS).

Les échanges entre les différentes zones de sécurité sont systématiquement contrôlés par des firewalls appliquant le principe élémentaire « tout ce qui n'est pas explicitement autorisé est interdit ». Le filtrage est de type stateful (contrôle source/destination/protocole) et les flux sont journalisés.

Sécurité des flux client

Les clients se connectent aux environnements Cloud Avenue à des fins d'administration ou d'accès aux services. Les flux d'administration des clients sont systématiquement sécurisés par des protocoles garantissant l'authentification, la confidentialité et l'intégrité (TLS,

AES256…). Les méthodes d'accès varient selon les offres et les options sélectionnées par le client.

La sécurité des flux de service dépend de l'offre considérée, mais de manière générale, les échanges sont sécurisés avec des connexions de type SSL/TLS qui respectent l'état de l'art du moment.

3.9.3. Protection contre les dénis de service et les intrusions

Orange Business dispose de protections pour protéger ses clients contre les attaques en déni de services :

- **Sondes de blackholing déployées au cœur du réseau du Groupe Orange**

  Cloud Avenue bénéficie d'un système de protection contre les attaques massives en déni de service provenant d'Internet. Ce système est déclenché par le Security Operating Center (SOC) d'Orange en s'appuyant sur des sondes déployées en cœur du réseau opérateur du Groupe Orange.

  La solution offre deux niveaux de service, l'un fourni en standard, l'autre optionnel :

  - L'activation d'une fonction de type "trou-noir"/"blackholing". Cette solution rend les adresses IP attaquées injoignables depuis Internet les adresses IP attaquées et protège les autres clients du Cloud Public contre les effets de bord potentiels, comme les baisses de performance de la bande passante Internet. Elle est incluse par défaut dans les services opérés depuis des centres d'hébergement Orange en France.
  - Le re-routage des flux vers un centre de nettoyage temps-réel pour ensuite réinjecter le trafic sain aussi appelé « cleanpipe ». Cette solution est un service d'Orange Cyberdefense optionnel payant.

- **Pare-feux situés à l'entrée des plateformes Cloud Orange**

  Le trafic en entrée de plate-forme est supervisé par des pare-feux qui filtrent certains paquets jugés suspects par simple analyse protocolaire, par exemple :

  - Protocoles IP : SYN Flood, UDP Flood, ICMP Flood, Land Attack, ICMP fragment, Large ICMP packets, SYN fragments.
  - Flux applicatifs : les pare-feux sont également capables de détecter des attaques spécifiques sur certains protocoles applicatifs : DNS, FTP, http, REAL, RSH, RTSP, TALK, TFTP, XING…

  NB : Cette fonction dite de screening n'apporte pas de protection avancée contre les intrusions ou les attaques applicatives. Des solutions d'Orange Cyberdefense peuvent être proposées pour adapter la protection à la criticité des données et du service du client.

3.10. Acquisition, développement et maintenance des systèmes d'information

Ce chapitre correspond à la thématique 14 de l'ISO 27002 version 2017.

3.10.1. Analyse de risques

L'analyse de risque est la base du système de gestion de la sécurité de Global Delivery & Operations. Des experts sécurité formés à l'analyse de sécurité de type ISO27005 ou EBIOS mènent de nombreuses analyses de risque sur le périmètre de responsabilité d'Orange. Le principe de fonctionnement de ces dernières est détaillé ci-dessous :

- Analyse de risque annuelle du système de management de la sécurité (SMSI) : dans le cadre de la certification ISO27001, une analyse de risque globale des principaux services, processus et outils de Global Delivery & Operations est réalisée, avec un plan de traitement de risque validé par le directeur exécutif de Global Delivery & Operations ;
- Analyse de risque de haut-niveau (HLRA : High-Level Risk Analysis) avant chaque démarrage de nouveau service/solution : cette analyse de risque permet d'évaluer les principaux risques (données personnelles, etc.) et orienter très en amont les équipes projet vers des solutions ;
- Analyse de risque de sécurité (Security Risk Analysis) : selon les résultats du HLRA, une analyse de risque complète de sécurité est menée ou non. Cette analyse de risque permet d'identifier les risques liés à l'architecture, au modèle opérationnel et à l'organisation ;
- Analyse de risque dans le cas d'une « due diligence » : vérification de la sécurité d'un fournisseur de solution ou de sous-traitance, voire en cas d'acquisition de société.

Les analyses de risques proposent systématiquement des mesures de sécurité à mettre en place pour limiter les risques identifiés. Ces documents ne sont pas transmis aux clients pour des raisons de confidentialité.

3.10.2. Bonnes pratiques de développement et d'intégration

Bonnes pratiques de développement

Les développements spécifiques réalisés par Orange ou par un sous-traitant respectent le guide interne Orange de bonnes pratiques de développement sécurisé (constitué de 38 mesures).

Bonnes pratiques d'intégration / renforcement de la sécurité des configurations

Les systèmes et logiciels sous la responsabilité d'Orange sont configurés avec un niveau de sécurité renforcé par l'application d'un « guide de hardening ». Par exemple pour les environnements VMware vSphere, Orange se base sur les guides de hardening sécurité fournis par VMware (https://www.vmware.com/security/hardening-guides.html).

Certification sécurité des composants critiques

Le Centre de Compétence Sécurité Cloud d'Orange veille à ce que les composants critiques aient des certifications de sécurité reconnues sur un périmètre approprié avant d'être intégrés dans nos offres Cloud. Ainsi, le Centre de Compétence Sécurité Cloud s'appuie généralement sur les certifications « Critères Communs » (ISO 15408) et vérifie leur pertinence en contrôlant les paramètres suivants :

- Niveau d'assurance : EAL4 souhaité au minimum.
- Cible de sécurité couvrant des domaines fonctionnels suffisamment larges : support cryptographique, identification et authentification, étanchéité des machines virtuelles...

A titre d'exemple, les composants critiques suivants sont certifiés critères communs :

- VMWare : https://www.vmware.com/fr/security/certifications/common-criteria.html
- Pare-feu Juniper : EAL4.

3.10.3. Recette de sécurité

Validation sécurité des composants

Les composants les plus critiques de la plateforme de Cloud Avenue font l'objet de tests de sécurité (revue de configuration/code et/ou tests d'intrusion) afin de valider leur niveau de sécurité.

A titre d'exemple, les portails d'administration ont déjà fait plusieurs fois l'objet de plusieurs tests d'intrusion et d'une revue de configuration/code.

Tous les templates (OS ou applicatifs) fournis par Orange font également l'objet d'une validation et sont régulièrement testés et mis à jour pour prendre en compte les dernières vulnérabilités et patchs.

Plateforme de non-production

Des plateformes de développement/qualification/préproduction existent, notamment pour valider la sécurité des évolutions ou pour mener des audits complets d'intrusion.

En cas de déploiement de patch ou de nouveaux services, ces derniers sont d'abord testés sur ces plateformes de non-production afin de valider le bon fonctionnement et les non-régressions du patchs et/ou des nouveaux services.

Absence de données clientes sur les plateformes de non-production

Aucune donnée cliente n'est présente sur les plateformes de non-production qui sont complètement disjointes des plates-formes de production.

3.11. Gestion des sous-traitants

Ce chapitre correspond à la thématique 15 de l'ISO 27002 version 2017.

3.11.1. Sécurité dans les contrats avec nos sous-traitants

Dans le cadre du référencement, Orange évalue la gestion de la sécurité de ses principaux fournisseurs avec notamment la fourniture d'un plan d'assurance sécurité détaillant les mesures prises par l'entreprise pour garantir la sécurité de la prestation réalisée pour Orange.

L'acceptation des équipes de la sécurité interne fait partie des prérequis au référencement.

Nos prestataires/fournisseurs s'engagent dans nos contrats sur la confidentialité et l'intégrité des données qu'ils auront à leur connaissance durant la prestation.

Les sous-traitants intégrés aux équipes internes Orange utilisent les mêmes outils et processus que les personnels Orange, et respectent donc par défaut les bonnes pratiques explicitées dans ce document : sensibilisation, contrôle d'accès physique et logiques …

3.11.2. Suivi de la sécurité des services fournis par nos sous-traitants

Orange prévoit la possibilité d'auditer ses sous-traitants afin de vérifier le respect des engagements sécurité prévus dans les contrats. Ces audits débouchent sur des plans d'actions sécurité permettant d'améliorer le niveau de sécurité des sous-traitants.

3.12. Gestion des incidents de sécurité

Ce chapitre correspond à la thématique 16 de l'ISO 27002 version 2017.

La politique de gestion des incidents de sécurité est décrite dans le chapitre 12 de la politique de sécurité Orange Cloud for Business « OCB Security Policy v1.6 ».

Elle est déclinée dans le chapitre 4 du processus de gestion des incidents « [4] ». Le présent chapitre explicite les principes décrits dans ces documents.

Préparation des équipes opérationnelles

Cette phase a pour but de préparer chaque intervenant au traitement des incidents : excellence opérationnelle (sensibilisation, entrainements réguliers à la gestion des différents types d'incidents…) et accès rapide à une documentation à jour (inventaire des actifs, schéma réseau, documentation technique, journaux…).

Lors de cette préparation, les opérationnels sont sensibilisés à l'identification d'incidents de sécurité potentiels. Le principe est que lorsqu'un incident opérationnel est identifié alors l'opérationnel en charge puisse identifier de manière raisonnable si l'incident peut entrainer un problème de sécurité (typiquement si un système de protection tombe en panne) ou si

l'origine de l'incident peut être liée à la sécurité (malware, botnet, tentative d'intrusion, déni de service ...).

Détection des incidents de sécurité

Les moyens de détection mis en œuvre pour détecter un incident de sécurité sont :

- Outils de supervision standards (Patrol, shinken) ou spécifiques à la sécurité (SIEM[12], sondes anti-DDOS) ;
- Personnel en charge de la supervision des journaux (IDS, log FW, log systèmes, log applicatifs…) ;
- Cellule de veille ;
- Equipe sécurité (ex : Centre de Compétence Sécurité Cloud) ;
- Alertes remontées par le client.

Cette supervision s'effectue sur les composants sous la responsabilité directe d'Orange (portail, hyperviseur, environnements clients dont la sécurité est managée par Orange…).

Enregistrement et qualification des incidents de sécurité

Orange Business dispose d'un outil de gestion des incidents de sécurité.

Les alertes sont saisies dans l'outil sous forme d'un ticket d'incident par deux types d'acteurs :

- Les acteurs techniques en charge de l'exploitation / supervision du service ;
- Les acteurs du centre de support, alertés par un appel ou un mail du client.

Les alertes sont qualifiées selon leur nature et leur gravité.

Nature de l'incident - L'outil de gestion des incidents distingue quatre catégories d'incidents :

- Intrusion ;
- Dysfonctionnement ;
- Vulnérabilité ;
- Légal (incident de nature réglementaire faisant intervenir des acteurs particuliers).

Gravité de l'incident - Le tableau ci-dessous synthétise les niveaux de gravité des incidents ainsi que les actions à mener :

Niveau	Description
1	**Critique** Perte complète des services pour plusieurs utilisateurs, ou incident ayant un impact critique sur les activités du client. Nécessite une prise en compte immédiate et la mise à disposition en urgence de ressources dédiées jusqu'à résolution de l'incident.
2	**Majeur** Services dégradés. Les utilisateurs peuvent accéder aux services mais connaissent des difficultés ou subissent des délais significatifs. Nécessite une prise en compte immédiate et la mise à disposition de ressources pour une résolution rapide de l'incident.

[12] SIEM : Security Information Event Management, outil permettant de corréler les logs, c'est-à-dire de relier des évènements différents à une même cause.

3	**Mineur** Services fournis avec des délais ou des difficultés mineurs. L'activité de l'entreprise n'est pas significativement entravée. Nécessite une prise en compte programmée pour éviter toute dégradation significative du service.

Le ticket d'incident est aiguillé vers l'équipe adéquate incluant le Centre de Compétence Sécurité Cloud.

Réponse à l'incident de sécurité

Les réponses suivantes peuvent être apportées :

- Mesures d'urgence (mise en quarantaine, …) ;
- Activation de la cellule de crise ;
- Communications aux clients, aux partenaires, aux exploitants ;
- Application d'un correctif ;
- Restauration d'un système ;
- …

Revue et actions post-incident

Une fois l'incident de sécurité traité, le Centre de Compétence Sécurité Cloud analyse la nature de l'incident et la qualité de la réponse apportée par Orange. Si besoin, le Centre de Compétence Sécurité Cloud met à jour les procédures de gestion des incidents de sécurité dans une démarche d'amélioration continue.

Communication vers les clients

Pour les incidents ayant pu avoir un impact sur la sécurité des clients d'Orange, une communication est faite vers les clients selon les modalités prévues au contrat. Pour les clients ayant opté pour un Business Security Officer dédié, la communication se fera directement vers le RSSI du client.

3.13. Sécurité de la gestion de la continuité d'activité

Ce chapitre correspond à la thématique 17 de l'ISO 27002 version 2017.

Les taux de disponibilité de chaque offre sont précisés dans les descriptions de services.

Toutes nos offres Cloud ont leur infrastructure entièrement redondée sur plusieurs sites (ou par exception temporaire sur plusieurs salles informatiques), avec des mécanismes de haute disponibilité de manière à rendre transparent les pannes locales : réseau (accès Internet, accès VPN, pare-feu), portail d'administration, virtualisation, stockage…

Toutes les sauvegardes (configuration, sauvegardes clients) sont répliquées sur des sites distants afin de garantir la disponibilité des données en cas de sinistre majeur sur le site de production.

Les offres Cloud Avenue sont exploitées depuis plusieurs plateaux d'exploitation, comme explicité dans la partie 3.7. Ainsi, en cas d'indisponibilité total d'un site d'exploitation, la continuité de l'administration des offres Cloud Avenue est assurée.

La continuité de l'exploitation est régulièrement testée au travers de simulations.

Des clauses de réversibilité sont présentes dans les contrats des offres Cloud Avenue. En cas de résiliation du Service, à l'exception de la résiliation pour faute du Client, le Client pourra demander à Orange Business le déclenchement de la réversibilité. Orange Business mettra alors en œuvre les moyens raisonnablement nécessaires pour assurer la continuité du Service, afin que le client dispose, à l'issue de la Période de Réversibilité, des capacités lui permettant de continuer à satisfaire ses besoins (cf. contrat plus de détails).

3.14. Conformité

Ce chapitre correspond à la thématique 18 de l'ISO 27002 version 2017.

3.14.1. Respect des exigences légales et contractuelle

Dans le cadre de la démarche d'analyse de risques propre à tout projet d'Orange, une revue des obligations légales et contractuelles est effectuée et un plan d'action est proposé. Le livrable produit s'appelle le LOA (Legal Obligation Assessment). Les points abordés sont :

- Le respect des clauses contractuelles (licences, propriétés industrielles, engagements spécifiés dans la description de service…) ;
- Le respect des réglementations spécifiques issues du domaine d'activité d'Orange (LCEN[13] et CPCE[14]) ;
- La tenue d'un registre des traitements de données à caractère personnel, conformément au Règlement général sur la protection des données (RGPD). Orange Business Services a nommé un DPO (Data Protection Officer, ou délégué à la protection des données) qui assure la tenue du registre. Le DPO est un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable des traitements de ces données, que dans les rapports de ce dernier avec la CNIL (Commission Nationale de l'Informatique et des Libertés), autorité administrative indépendante chargée de veiller au respect du RGPD. Le DPO occupe ainsi une place centrale dans le développement sécurisé des nouvelles technologies de l'information et de la communication et assure, au sein de l'entreprise, la diffusion

[13] LCEN : Loi pour la Confiance dans l'Economie Numérique
[14] CPCE : Code des Postes et des Communications Electroniques

de la culture informatique et libertés et la maîtrise des risques sur les données à caractère personnel ;

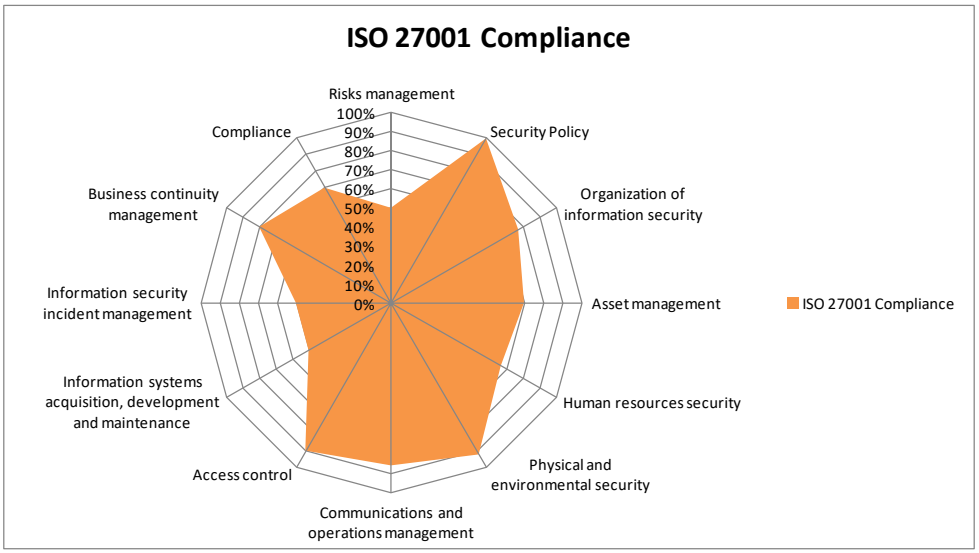
- Le respect des exigences de l'ANS[3] pour les offres certifiées Hébergeur de données de santé ou disposant d'un agrément Santé (à savoir Health Data Solutions).

Toujours dans ce même cadre d'analyse de risque, une revue des données personnelles est proposée. Le livrable produit s'appelle le PRA (Privacy Risk Assessment).

3.14.2. Contrôle du respect des politiques de sécurité

Le Centre de Compétence Sécurité Cloud a la charge de contrôler l'application de la Politique de Sécurité pour chaque offre Cloud. Il réalise donc un contrôle continu et pilote des audits organisationnels et techniques à minima tous les 6 mois sur des périmètres tournants.

- Exemple d'audit organisationnel : contrôle de la gestion des habilitations ;
- Exemple d'audit technique : tests d'intrusions, réalisation de scan Nessus ou Qualys, audit de configuration…



Exemple de bilan de maturité ISO 27001 (valeurs mises à titre d'exemple)

En complément, Orange Business est soumis à des audits réguliers (AFNOR, ISAE 3402) réalisés par des organismes externes et menant à des contrôles du niveau de sécurité.

3.14.3. Certifications liées à la sécurité

Orange possède les certifications suivantes adhérentes au périmètre des offres Cloud :

- ISAE 3402 pour les centres d'hébergement
  - Les centres d'hébergement d'Orange sont certifiés ISAE 3402 Type II (ex SAS70).

- Certification sécurité ISO 27001
  - Orange Business possède une certification sécurité ISO 27001 sur le périmètre de la « mise en œuvre, la fourniture et le support de services en infogérance et de solutions de communications » pour les sites de Cesson-Sévigné, d'Egypte, de l'île Maurice et de l'Inde[15].
- Agrément Santé délivré par le gouvernement Français (organisme ASIP Santé)
  - Dans le cadre de nos offres de Cloud public de type IaaS, l'offre " Health Data Solutions" bénéficie d'un "Agrément Santé".
- Certification Critères Communs EAL 2+ (ISO 15408) sur la sécurité du réseau international IP-VPN en 2008
  - Le rapport de certification est disponible ici : http://www.ssi.gouv.fr/IMG/certificat/dcssi_2008-20fr.pdf
  - La cible de certification est disponible ici : http://www.ssi.gouv.fr/IMG/certificat/dcssi-cible_2008-20fr.pdf
- Certification Critères Communs (ISO 15408) des équipements de sécurité et les équipements de virtualisation utilisés sur nos offres :
  - VMWare : https://www.vmware.com/security/certifications/common-criteria.html
  - Pare-feu Juniper : EAL4.

[15] Certificat associé : https://certificats-attestations.afnor.org/certification=335181233155

V

ANNEXES

A. Classification TIER d'un centre d'hébergement

La classification des datacenters par l'Uptime Institute constitue actuellement la seule base référentielle reconnue au niveau mondial : elle définit la performance, en termes de continuité de services, de l'infrastructure technique d'un datacenter.
Cette classification est volontairement simplifiée en cinq grands niveaux (appelés tier en anglais), présentés dans le tableau suivant, correspondant à la fois à des grandes catégories d'infrastructures, des époques initiales de déploiement et des capacités d'accueil en termes de charge électrique (W/m2).
Chaque niveau est affecté d'un indice de disponibilité statistique, basé sur l'historique de fonctionnement de dizaines de datacenters majeurs ainsi que sur des études de fiabilité établies grâce à des logiciels experts.

	TIER I	**TIER II**	**TIER III**	**TIER III+**	**TIER IV**
Source de remplacement (1)	1 GE	1 GE	1 GE	1 GE	2 GE ou (N+1) GE
Énergie primaire	1 voie active	1 voie active	1 voie active et 1 voie passive	Puissance nominale après un défaut majeur	Puissance nominale après un défaut majeur
Énergie Haute Qualité	1 voie active	1 voie active	1 voie active et 1 voie passive	2 voies actives	2 voies actives
Redondance sur la Haute Qualité	N	N+1	N+1	2N ou 2(N+1)	2N ou 2(N+1)
Maintenable sans arrêt d'exploitation	non	non	oui	oui	oui
Niveau de charge maximal (Watt/m²)	250 W/m²	500 W/m²	1000 W/m²	>1000 W/m²	>1000 W/m²
Taux de disponibilité **théorique**	99,671%	99,749%	99,982%	99,990%	99,995%
Nombre d'heures maximum d'arrêt du service par an **moyenné sur plusieurs années et plusieurs datacenters**	28,82 h/an	21,98 h/an	1,58 h/an	0,87 h/an	0,44 h/an

(1) GE = Groupe électrogène

Les infrastructures mises en place par France Télécom dans ses datacenters de génération 2004-2010 correspondent à un niveau de classification TIER III+. Les datacenters de dernière génération, construits après 2010, sont en tier IV. Pour certains, les installations de climatisation sont équipées de la fonction free-cooling.
Les datacenters OBS, conçus et utilisés pour l'offre hébergement, sont classifiés au minimum « TIER III ».