Évaluation de la sécurité de nos fournisseurs IT dans le cadre du référencement Groupe

Jean-Philippe Gaulier
Cécile Lesaint

05/10/2015

Les constats

- on découvre en permanence des failles OWASP dans nos applications en production
- une grande part de nos applications est sous-traitée (en développement, TMA, qualification)
- nos fournisseurs nous font payer la correction des failles !!!!

Les constats

aout 2014 - avertissement de la CNIL
en réponse à l'incident du mois d'avril

CNIL.

Délibération de la formation restreinte n° 2014- 298 du 7 août 2014 prononçant un avertissement à l'encontre de la société ORANGE

Enfin, la délégation a constaté que si la société avait encadré contractuellement ses relations avec son premier sous-traitant, elle n'avait en revanche pas veillé à ce que les obligations en matière de sécurité et de confidentialité des données soient répercutées au prestataire secondaire alors même qu'elle connaissait le périmètre d'intervention de ce dernier.

La formation restreinte retient qu'en sa qualité, par ailleurs non contestée, de responsable de traitements, la société a l'obligation d'assurer la sécurité et la confidentialité des données à caractère personnel de ses clients et prospects et qu'elle ne saurait minimiser sa responsabilité par le recours à plusieurs prestataires.

http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf

Chronologie des actions Groupe (ITNSEC, IST, GSSC)

Renforcement du contrat

mis en place sur les contrats groupe

livrable de qualité = livrable sans vulnérabilité

- ✓ collaborateurs formés
- ✓ procédures
- ✓ tests des livrables
- ✓ adaptation au type de prestation
- ✓ contrôlé

correction sans surcoût des vulnérabilités connues avant la livraison

Exemple : ITServices - les points clés

L'assistance technique

- Respect de nos procédures et politiques de sécurité
- Informer en cas de difficulté
- L'intervenant est sensibilisé à la sécurité
- Il est formé aux bonnes pratiques de sécurité de son métier
- La société s'engage à retourner en fin de mission tout bien (clé USB, ordinateur, téléphone, cartes SIM…) qui lui aura été confié . elle doit vous faire signer PV de réception et restitution. Vous devez également le faire pour le compte d'Orange
- La société nous fournit une matrice de contacts et nous informe de tout changement

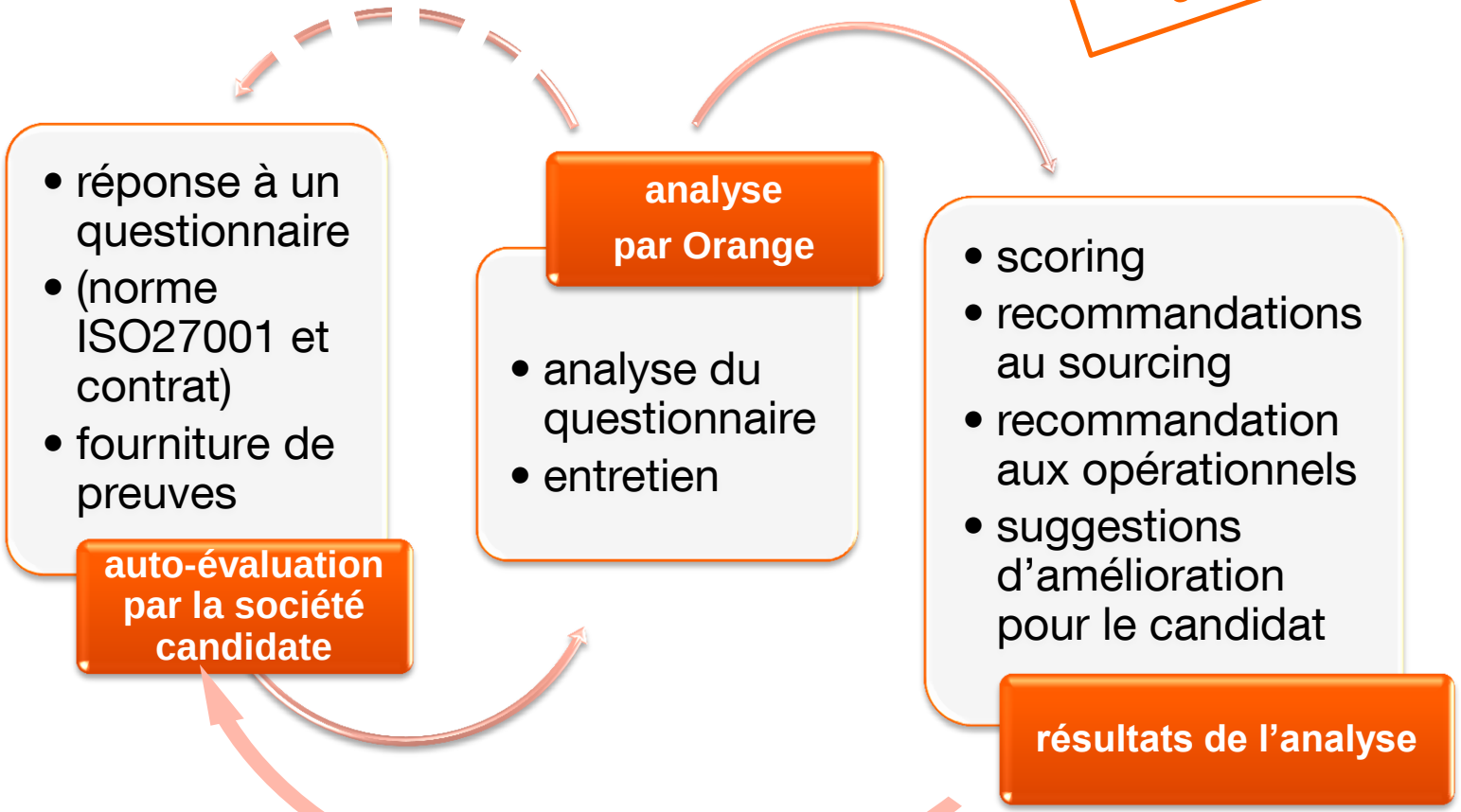
Le forfait

- Correction sans surcout et sans délais des failles dont le type est connue (avant la recette)
- Test (sécurité) et documentation des livraisons
- Prise en compte de notre classification de l'information
- Définition d'un niveau de confidentialité par défaut qui implique chiffrement et authentification forte)
- Mise en œuvre de l'interconnexion conforme au cahier des charges (politique, recette et tests conformité réguliers)
- Contrôle d'accès
- Protection des données personnelles
- Informer orange en cas d'incident et mobiliser les ressources nécessaires
- Indicateurs et revue de sécurité annuellement

Évaluation de la maturité sécurité du fournisseur

basée sur une autoévaluation de la société
par rapport à la norme ISO27001 et au contrat Orange

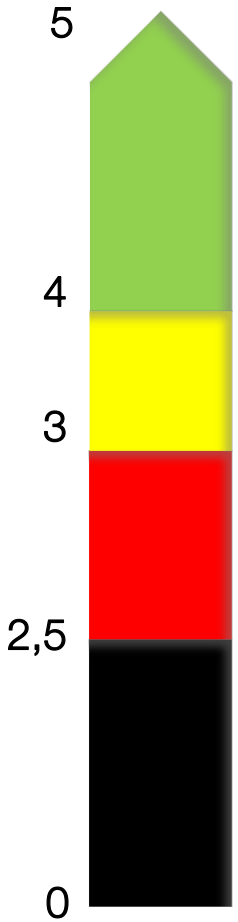
mis en place sur les contrats groupe



réévaluation sur demande du fournisseur
si progrès en cours de contrat (périodicité > 6mois)

L’échelle pour la notation des fournisseurs et les consignes

Source : ANSSI Maturité SSI – Approche méthodologique / ISO/IEC 21827

maturité du fournisseur	échelle	consigne
5 = Le niveau requis de la Sécurité est atteint, prouvé et contrôlé et optimisé (ce qui suppose expérience et antériorité)		Convient pour les projets standards et sensibles
Le niveau requis de la Sécurité est atteint, prouvé, et contrôlé en interne par le fournisseur.		
Le niveau requis de la Sécurité est atteint et prouvé.		Convient pour les projets standards ne convient pas pour les projets sensibles
Volonté d’atteindre la conformité - Le niveau requis de la Sécurité n’est pas atteint.		ATTENTION: ne convient pas pour des projets standards ou sensibles
Pas d’organisation globale de la sécurité, pas de culture du risque, très peu de pratiques		
0 = Pas de réponse, pas d’évaluation		

le livrable de l'évaluation : la scorecard sécurité

COMPANY

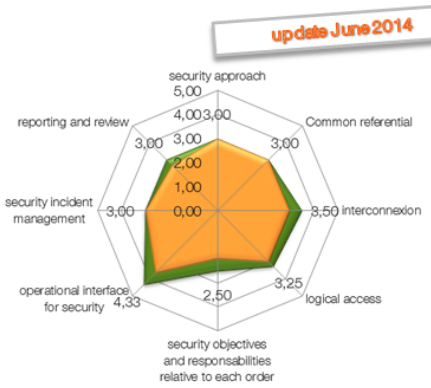
supplier ISO27001 partially certified

Final scorecard

TPAS AM	TPAS IM	ITServices Time&Material	ITServices Fixed Prices	ISO27002 best practices	verification score /2	confidence score %
NA	NA	3,1	2,9		1,32	80%

IT Services Time and Material scoring

update June 2014



IT Services Fixed Prices scoring

Legend

- supplier auto-assessment against ITServices contractual requirements
- what could be confirmed by the details and evidences provided

comment

areas for improvement:

- data protection (encryption tools and process, authentication tools and process, anonymization) : currently only options
- training on job security best practices,
- improve control on procedures in order to be able to apply for sensitive projects

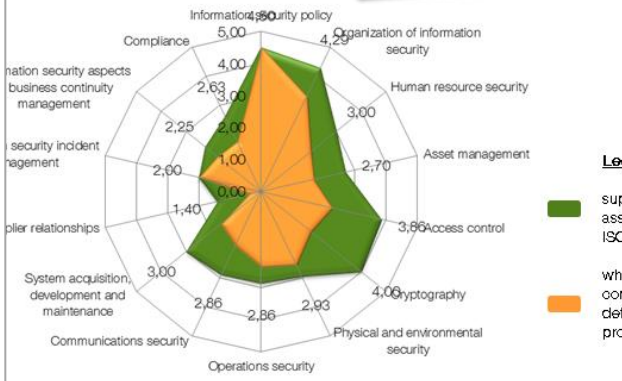
1

Orange confidential

Final scorecard

TPAS AM	TPAS IM	ITServices Time&Material	ITServices Fixed Prices	ISO27002 best practices	verification score /2	confidence score %
NA	NA	3,1	2,9		1,32	80%

update June 2014



IT Services SoA scoring per ISO category

Legend

- supplier auto-assessment against ISO27002
- what could be confirmed by the details and evidences provided

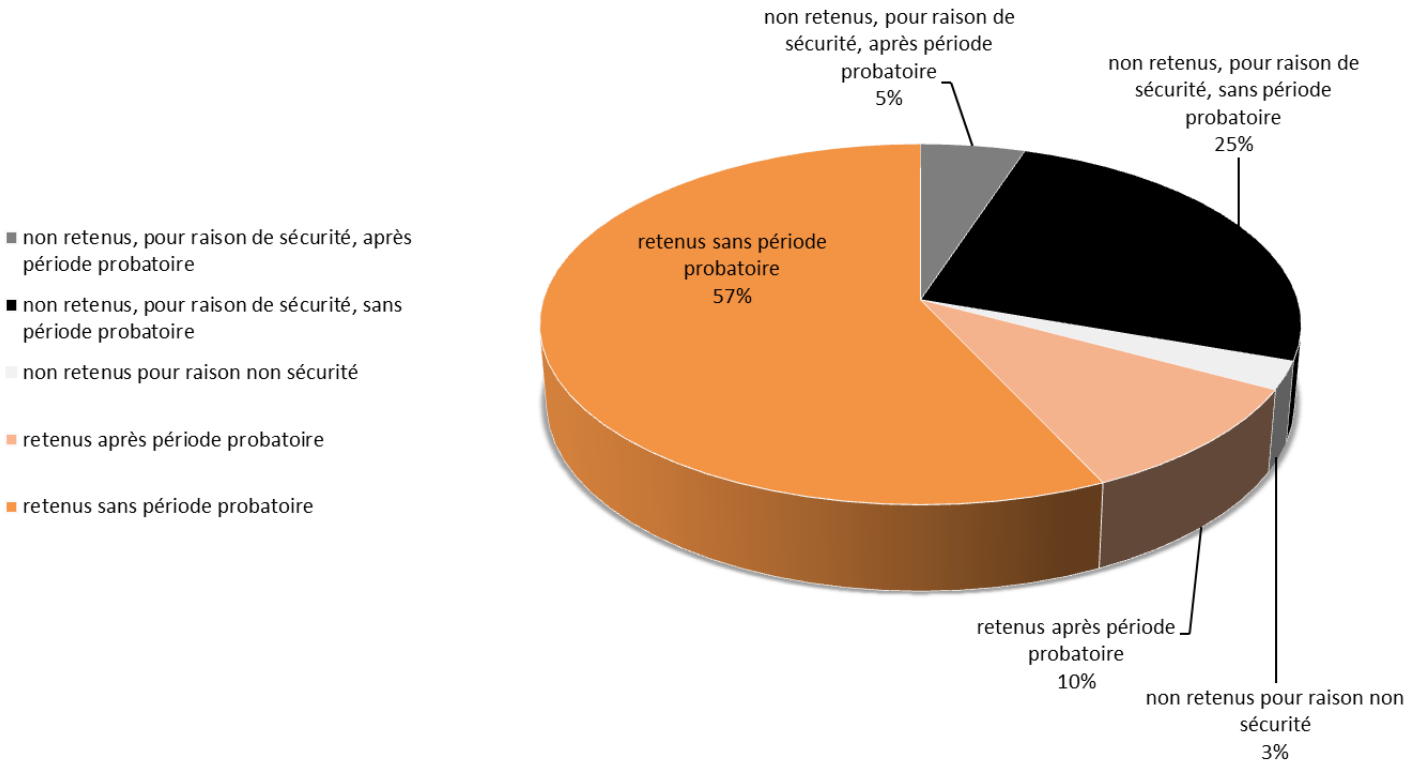
comment

certified on Morocco sites. Global certification planned for end 2016

2

Orange confidential

Statut octobre 2015 : la sécurité un critère de sélection dans le référencement Groupe



80 sociétés évaluées en 2 ans (TPAS, IT Services)

Consignes de choix des fournisseurs selon la sensibilité des nouveaux projets

mis en place sur les contrats groupe

réaliser l'analyse de risques et en déduire la sensibilité du projet

- inventaire et niveau de sensibilité
- exigences spécifiques du projet
- sensibilité globale du projet

cahier des charges

choix du fournisseur

- projet standard : fournisseur au moins jaune
- projet sensible : fournisseur vert

exceptions :

demande d'utiliser une société qui n'est pas à niveau

- demande de dérogation auprès de la sécurité avec plan d'accompagnement de la société prestataire (*cf slide contact*)

Et après… c'est pas fini !
Le suivi de projet

proposé par le fournisseur
modèle de PAS pour info

- Plan d'Assurance Sécurité obligatoire
- Intégration de la sécurité dans le suivi du projet (COPIL… suivi des comptes et revues d'habilitations)

suivi au quotidien

- Vérification des livrables sécurité apportés par le fournisseur (PV d'audits, et revues de code, actions correctives)

coralys, audits

- **Orange** doit également faire ces tests en recette
- Communiquer de façon annuelle une consolidation des constats sur la partie sécurité des prestations

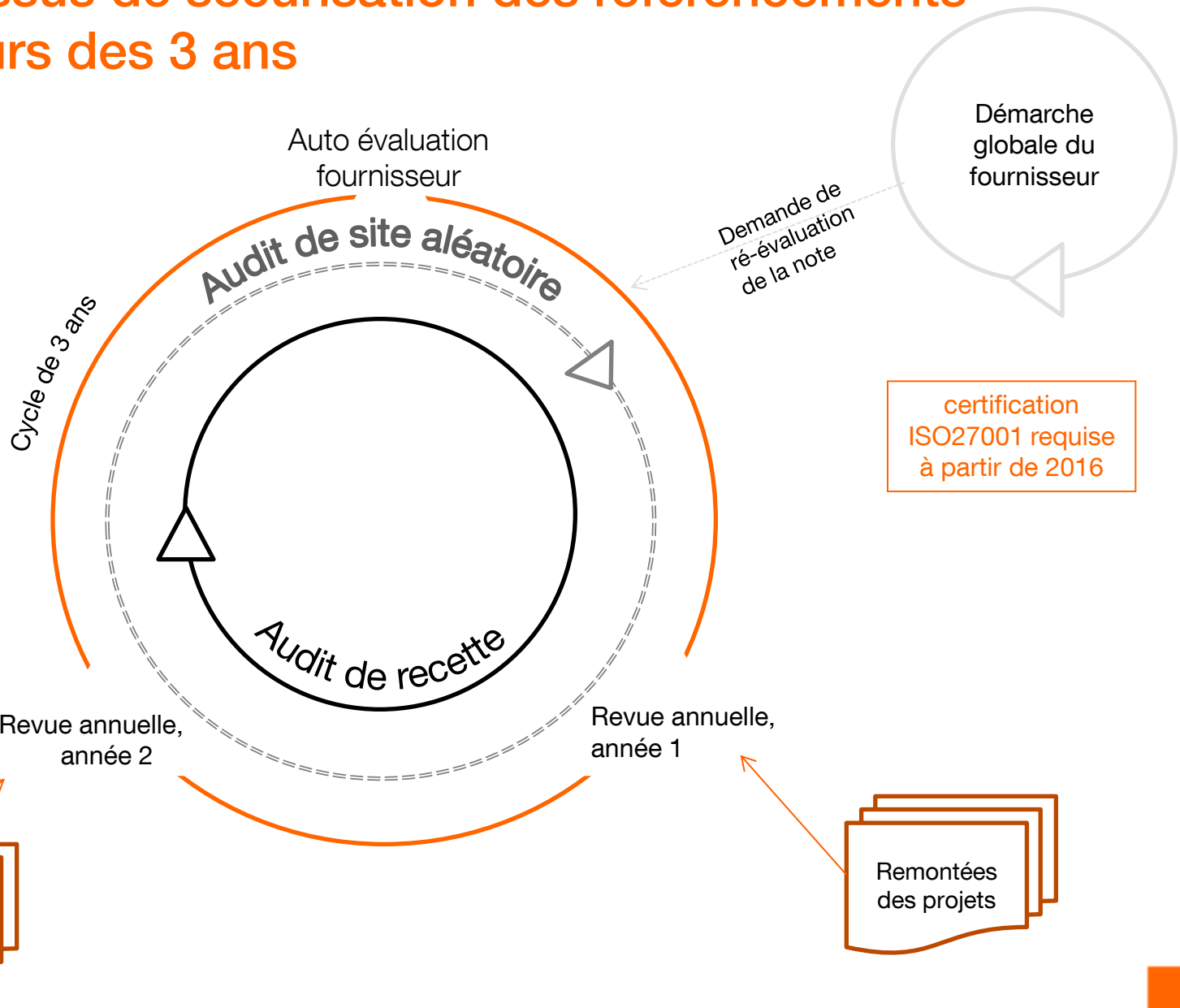
pour revues annuelles Groupe
transverses avec les fournisseurs

audits de contrôle sur site

- audits de conformité au contrat (exigences Orange et norme)
- sur site du fournisseur
- sur la base d'entretiens et de vérification de preuves
- établissement du programme d'audit sur des critères complémentaires
  - critère probatoire
  - degré de conviction à l'évaluation
  - retours projets
  - importance des projets sous-traité
  - incidents
  - ressenti lors des revues de sécurité
  - niveau de départ

  …

Processus de sécurisation des référencements au cours des 3 ans



Ressources humaines et temps nécessaire (étape d'évaluation)

- Un mois et demi pour répondre aux questions de l'auto-évaluation
- 3h d'entretien
- Deux semaines pour compléter les preuves

Pour les entreprises

- 4 ingénieurs SSI
- Connaissances achats et SSII
- Motivés…
- Une moyenne de 2000h de travail

Pour Orange

OUT OF SCOPE

- ✓ Préparation du processus
- ✓ Accompagnement du service achat
- ✓ Explication du processus aux sociétés

Contacts

IST/OPSIS

Cécile Lesaint
33 (0) 2 23 28 68 44
33 (0) 6 83 98 21 02
cecile.lesaint@orange.com

IST/OPSIS

Jean Philippe Gaulier
33 (0) 1 57 36 43 85
33 (0) 6 88 59 97 65
jeanphilippe1.gaulier@orange.com

merci