Analyse des risques

Version	1.3
Date	28/01/2014
Rédigé par	Pascal Edouard
Relu par	Julien Legras, Mathieu Latimier
Approuvé par	Ayoub Otmani

MISES À JOUR

Version	Date	Modifications réalisées
1.0	4/12/2013	Création
1.1	22/01/2014	Risque SSH
1.2	23/01/2014	Description de criticité
1.3	28/01/2014	Redéfinition des plans d'actions, et découpage des tâches d'absences

Table des matières

1 Objet

Document réunissant les différents risques qui pourraient arriver pendant ce projet ainsi que des plans d'actions pour les risques MAJEUR/CRITIQUE.

2 Terminologie et sigles utilisés

— Calcul de la criticité :

Afin de déterminer la criticité de chaque risque, une évaluation de la probabilité d'occurrence et de l'impact est estimé. La criticité est le produit de la probabilité de son occurrence par l'impact que le risque a sur le projet. On sera donc prêt pour appliquer les mesures adéquates face à ces risques.

CRITICITÉ = PROBABILITÉ × IMPACT

— Table des correspondances PROBABILITÉ/valeur et IMPACT/valeur :

Nom probabilité	**Valeur**		**Nom impact**	**Valeur**
FAIBLE	2		MINEUR	4
MAJEUR	3		MAJEUR	5
FORT	4		CRITIQUE	6

— Env : environnement
— RH : ressources humaines
— P : Pascal Edouard, J : Julien Legras, C : Claire Smets, W : William Boisseleau, M : Mathieu Latimier

3 Registre des risques

Réf.	Description	Facteurs	Type	Probabilité	Impact	Criticité
R01	Absences occasionnelles (quelques heures à une journée).	Entretiens, Administrations, Logement, Cours à l'INSAA pour William, Désagréments.	Humain	Fort	Mineur	16
R02	Absences prolongées sur plusieurs jours d'un ou plusieurs membres de l'équipe.	Accidents, Maladies, voyages à l'étranger imprévus.	Humain	Majeur	Majeur	15
R03	Programme de récupération des certificats ne fonctionne pas.	Mauvaise implémentation, bug intempestif, aucune connexion internet.	Technique	Faible	Majeur	10
R04	Programme de factorisation ne fonctionne pas.	Mauvaise implémentation, bug intempestif, ressources insuffisantes (mémoire, processeur, etc).	Technique	Fort	Majeur	20
R05	Perte des données.	Panne serveur GIT, récupération impossible des données depuis le serveur.	Technique	Faible	Majeur	10
R06	Récupération d'adresses IP impossible pour SSH.	Rapports d'abus.	Technique/Légal	Majeur	Majeur	15

4 Plans d'actions

Réf.	Action(s) prévue(s)	Action effectuée	Date	Par
R01	Soit l'absence ne génère pas de retard sur la tâche en cours (ou peut être rattrapée par les autres acteurs), soit la journée doit être rattrapée en cumulant plus d'heures dans la semaine.	Répartition des horaires de travail le jour même ou le samedi	20/01/14 (M) 22/01/14 (W) 23/01/14 (J) 27/01/14 (M) 28/01/14 (C)	Pascal
R02	Réorganisation et répartition de l'ensemble des tâches entre les membres restants de l'équipe.			Pascal
R03	Retravailler la structure du programme, répartir les bugs existant aux membres de l'équipe, changer de réseau.			Julien
R04	Retravailler la structure du programme, répartir les bugs existant aux membres de l'équipe, discuter d'une ressource disponible pour exécuter le programme de calcule.			Julien
R05	Faire une évaluation des données restants sur les machines de chaque membres de l'équipe et calculer les pertes de données.			William et Mathieu
R06	Arrêter temporairement le scan et décider avec le client de l'action à entreprendre.	Abandon de la partie SSH en accord avec le client.	21/01/2014	Claire

5 Annexes

5.1 Mail reçu le 19/01/2014 lié au risque R06

```
Dear Amazon EC2 Customer,

We've received a report that your instance(s):

Instance Id: i-6394312c
IP Address: 54.194.102.0

has been port scanning remote hosts on the Internet; check the information provided below by
the abuse reporter.

This is specifically forbidden in our User Agreement: http://aws.amazon.com/agreement/

Please immediately restrict the flow of traffic from your instances(s) to cease disruption to
other networks and reply this email to send your reply of action to the original abuse
reporter. This will activate a flag in our ticketing system, letting us know that you have
acknowledged receipt of this email.
```

```
It's possible that your environment has been compromised by an external attacker. It remains
your responsibility to ensure that your instances and all applications are secured.

Case number: 11135140320-1

Additional abuse report information provided by original abuse reporter:
* Destination IPs:
* Destination Ports: 22
* Destination URLs:
* Abuse Time: Sun Jan 19 11:36:00 UTC 2014
* Log Extract:
<<<
54.194.102.0 was observed probing caltech.edu for security holes. It
has been blocked at our border routers. It may be compromised.
...
```