PSSIE :
Pssi Sans Souffrance à l'IsaE

Yann Bachy - Laurent Dairaine

14 novembre 2017

jres Nantes 2017

La PSSI à l'ISAE

- Première PSSI rédigée en 2007
- Recrutement d'un nouvel OSSI en 2015

La PSSI à l'ISAE

- Première PSSI rédigée en 2007
- Recrutement d'un nouvel OSSI en 2015 *(moi...)*

La PSSI à l'ISAE

- Première PSSI rédigée en 2007
- Recrutement d'un nouvel OSSI en 2015

Découverte de la PSSIE

Une première tentative ...

```
ossi@isae:/# merge pssi_isae_v1.pdf pssie.pdf > pssi_isae_v2.pdf
```


IT'S
Easy

L'idée excellente du siècle !

Étudier chaque règle de la PSSIE en fonction d'un ensemble de critères

L'idée excellente du siècle !

Étudier chaque règle de la PSSIE en fonction d'un ensemble de critères

- Avec les acteurs des différents métiers impactés par les règles (logistique, infrastructure, poste de travail, applications métier, ...)
- Sessions d'environ 1h à 1h30 soient une dizaine de règles

Les critères

Pour chaque règle on étudie :

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;

  On cherche a évaluer à quel niveau [0-4] la règle est applicable à l'ISAE :
  - 0 : Pas applicable
  - 1 : Applicable à la marge
  - 2 : Moyennement applicable (ne pas utiliser)
  - 3 : Non applicable à la marge
  - 4 : Applicable complètement

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;

On cherche à évaluer le niveau de maturité de la mise en œuvre à l'ISAE par rapport au niveau d'applicabilité de la règle :

- 0 : Non traité
- 1 : Réalisé de manière exceptionnelle
- 2 : Conformité moyenne
- 3 : Non réalisé de manière exceptionnelle
- 4 : Conforme

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;

  On cherche à évaluer le risque présent lié à notre éventuelle non-conformité actuelle à une règle :
  - 0 : Aucun risque
  - 1 : Quelques risques résiduels
  - 2 : Risque moyen
  - 3 : Quelques réductions du risque
  - 4 : Risque total

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;
- le **budget** (€ et RH) estimé nécessaire à la mise en œuvre ;

  On cherche à évaluer un budget initial et récurrent pour la mise en œuvre de cette règle (précision +-30%) :
  - **budget initial** : le budget de mise en œuvre initial pour la mise en œuvre de la règle (en €).
  - **budget récurent** : le budget annuel de fonctionnement pour que la mise en œuvre de la règle reste utile (en €/an).

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;
- le **budget** (€ et RH) estimé nécessaire à la mise en œuvre ;
- la **mise en œuvre actuelle** ;

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;
- le **budget** (€ et RH) estimé nécessaire à la mise en œuvre ;
- la **mise en œuvre actuelle** ;
- les **actions à mener** afin d'atteindre les objectifs ;

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;
- le **budget** (€ et RH) estimé nécessaire à la mise en œuvre ;
- la **mise en œuvre actuelle** ;
- les **actions à mener** afin d'atteindre les objectifs ;
- les **risques assumés** ;

Une règle n'est pas toujours applicable dans le contexte spécifique de l'ISAE-SUPAERO. Les risques assumés identifient ce que la règle est supposée couvrir et ce qui ne sera pas couvert par le défaut d'applicabilité .

Les critères

Pour chaque règle on étudie :

- l'**applicabilité** de la règle à l'ISAE ;
- la **conformité** actuelle de la mise en œuvre ;
- le **risque résiduel** lié à notre éventuelle non-conformité ;
- le **budget** (€ et RH) estimé nécessaire à la mise en œuvre ;
- la **mise en œuvre actuelle** ;
- les **actions à mener** afin d'atteindre les objectifs ;
- les **risques assumés** ;
- éventuellement une **réécriture de la règle**.


MORTON
Coarse
KOSHER SALT
MORTON
Coarse
KOSHER SALT
market pantry
Ground
Black Pepper

INTERDIT AUX MOINS DE 10 ANS

kibana

REDMINE
flexible project management

Jenkins

elastic

Les règles dans redmine...

#	SOURCE (SSI)	SUJET	RÉFÉRENCE (SSI)	ACTEURS MÉTIER	CONFORMITÉ	APPLICABILITÉ (SSI)	RISQUE RÉSIDUEL (SSI)	STATUT
	01 - Politique, Organisation, Gouvernance (8)							
9309	PSSI-E	1.01 - Organisation SSI	ORG-SSI	DG, DG/OSSI, SG	2	4	0	Arbitrage
9310	PSSI-E	1.02 - Identification des acteurs SSI	ORG-ACT-SSI	DG, DG/OSSI, SG	3	4	0	Arbitrage
9311	PSSI-E	1.03 - Désignation du responsable SSI	ORG-RSSI	DG, SG	4	4	0	Terminé
9312	PSSI-E	1.04 - Formalisation des responsabilités	ORG-RESP	DG, DG/OSSI, SG	0	4	1	Arbitrage
9317	PSSI-E	1.05 - Gestion contractuelle des tiers	ORG-TIERS	DG/OSSI, SG, SG/AJ	0	4	3	Arbitrage

Une règle...

1.03 - Désignation du responsable SSI

« Précédent | 3 sur 183 | Suivant »

Ajouté par Yann BACHY il y a 8 mois. Mis à jour il y a 5 mois.

Statut:	Terminé		
Priorité:	Normal		
Assigné à:	Yann BACHY		
Version cible:	-		
Référence (SSI):	ORG-RSSI	**Risque résiduel (SSI):**	0
Section (SSI):	01 - Politique, Organisation, Gouvernance	**Actions à mener (SSI):**	
Objectif PSSI-E (SSI):	1 - Organisation de la SSI	**Applicabilité (SSI):**	4
Source (SSI):	PSSI-E	**RH initiale (j.h):**	0
Acteurs métier:	DG, SG	**RH réccurente (j.h/an):**	50
Budget initial (€):		**Risques assumés:**	
Budget réccurent (€/an):		**Mise en oeuvre actuelle:**	• L'OSSI est identifiés et opérationnel au sein de l'ISAE-SUPAERO
Conformité:	4	**Règle réécrite (SSI):**	

Workflow : Nouveau | Etude | Arbitrage | Planifié | En cours | Terminé


WHAT'S
NEXT?

Un document présentable ...

1.03 - Désignation du responsable SSI [ORG-RSSI]

Etude | Arbitrage | Planifiée | Réalisation | **Appliquée**

Normal | Applicabilité 4 | Conformité 4 | Risque résiduel 0

REGLE PSSI-E ORIGINALE

Chaque autorité qualifiée en sécurité des systèmes d'information (AQSSI) s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information (RSSI), chargé(s) de l'assister dans le pilotage et la gestion de la SSI. Des « correspondants locaux SSI » peuvent être désignés, le cas échéant, afin de constituer un relais du RSSI. Le RSSI d'une entité fait valider les mesures d'application de la PSSIE par l'autorité qualifiée et veille à leur application. Des dénominations alternatives des fonctions citées ci-
dessus peuvent être utilisées si nécessaire.

MISE EN OEUVRE ISAE-SUPAERO

Pilote : Yann BACHY avec l(es) entité(s) SG DG

Elements de mise en oeuvre opérationnels aujourd'hui :

- L'OSSI est identifiés et opérationnel au sein de l'ISAE-SUPAERO

Pas d'actions restant à mener.

Le cycle de vie d'une règle ...

Le cycle de vie d'une règle ...

- **Étude** : évaluation des critères pour chaque règle par une équipe de travail.

Le cycle de vie d'une règle ...

- **Étude** : évaluation des critères pour chaque règle par une équipe de travail.
- **Arbitrage** : validation par notre direction des résultats de la phase d'étude.
  Les points importants à valider lors de l'arbitrage :
  - l'**applicabilité** d'une règle : ce critère mesure le niveau de conformité que l'ISAE-SUPAERO vise à mettre en œuvre par rapport aux exigences de l'état. Lorsque ce critère est inférieur à 4, cela indique que nous visons un niveau de sécurité inférieur à celui préconisé par l'état, ce qui suppose l'acceptation de certains risques qui sont alors listés dans la rubrique des "Risques assumés",
  - les coûts (Financiers et RH, initiaux et récurrents) : La mise en œuvre liée à certaines règles nécessites des coûts plus ou moins importants. Les valeurs présentés sont une estimation à 30%.

Le cycle de vie d'une règle ...

- **Étude** : évaluation des critères pour chaque règle par une équipe de travail.
- **Arbitrage** : validation par notre direction des résultats de la phase d'étude.
- **Planifié** : projet validé par la direction, intégration dans le système de gestion par projet du SI.

Le cycle de vie d'une règle ...

- **Étude** : évaluation des critères pour chaque règle par une équipe de travail.
- **Arbitrage** : validation par notre direction des résultats de la phase d'étude.
- **Planifié** : projet validé par la direction, intégration dans le système de gestion par projet du SI.
- **En cours** : mise en œuvre en cours par le SI (ou autre entité responsable).

Le cycle de vie d'une règle ...

- **Étude** : évaluation des critères pour chaque règle par une équipe de travail.
- **Arbitrage** : validation par notre direction des résultats de la phase d'étude.
- **Planifié** : projet validé par la direction, intégration dans le système de gestion par projet du SI.
- **En cours** : mise en œuvre en cours par le SI (ou autre entité responsable).
- **Appliqué** : règle entièrement appliquée.


That's all Folks!