Démarche PSSI générique : retour d'expérience d'établissements pilotes

Bernard Martinet
Annie Cobalto
Dominique Launay
Roger Négaret

Plan

- Synthèse des 7 projets établissements
- Les livrables du projet
- Focus sur 3 établissements

Synthèse des 7 projets en établissement

- Les établissements
  - Université de la Méditerranée (Aix-Marseille Université)
  - Université de Bordeaux 1
  - Université de Limoges
  - Université de Nancy (PRES Université de Lorraine)
  - Université de Rennes 1
  - Université de Grenoble (PRES)
  - Réseau Universitaire Numérique Normand (UNR)

Synthèse : organisation projet

Pour chaque établissement

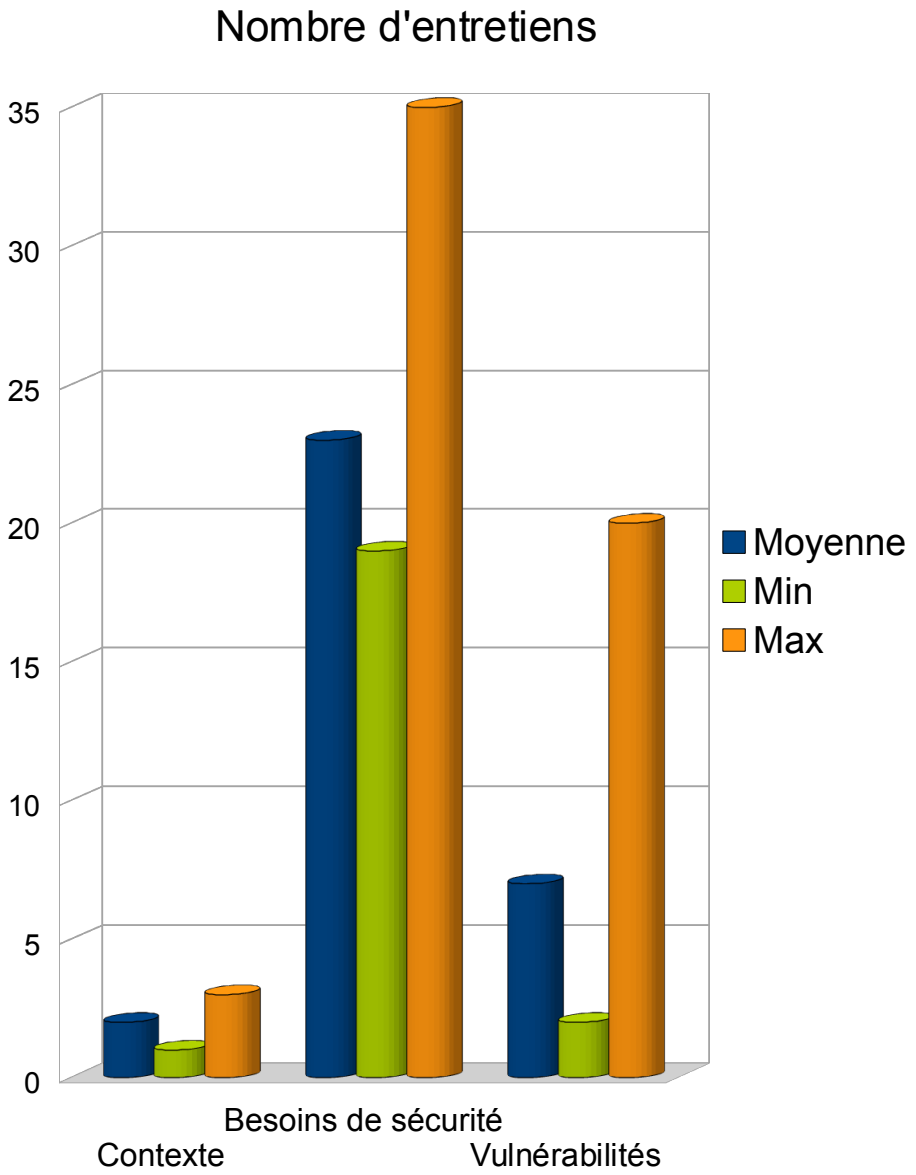
Équipe projet (3 à 6 personnes)	• Entretiens • Cartographie • Validation • ...
Comité de pilotage	• Spécifique ou • Basé sur un comité existant

Structure classique mais indispensable à la réussite du projet

Synthèse : Analyse de Risques

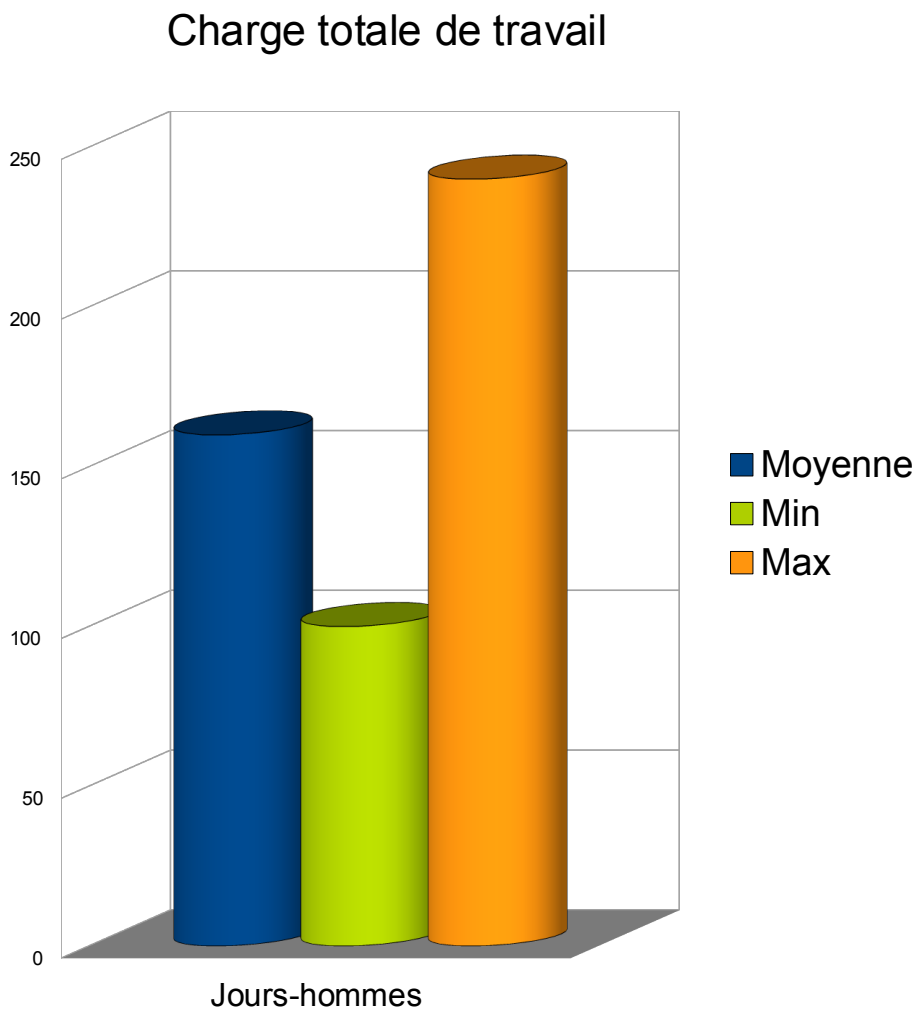
- Durée : 1 à 4 mois (2,5 en moyenne) pour entretiens, menaces, risques
- Les entretiens
  - durée 1h à 2h (1h30 en moyenne)
  - ½ à 1 journée avec préparation, analyse, mise en forme, validation
  - réalisés la plupart du temps en tandem au niveau de l'équipe projet

Synthèse : Entretiens



- Phase essentielle de l'analyse de risques :
  - rencontre des acteurs au plus haut niveau de la gouvernance
  - l'interlocuteur doit être choisi en fonction de l'entretien (contexte, besoins de sécurité, vulnérabilités)
- Occasion de sensibiliser les acteurs à la SSI dans leur métier

Synthèse : Charge de travail



- Non compris :
  - temps passé dans le groupe de travail national
  - temps de formation
  - temps de validation final des documents
- Fonction de :
  - structure de l'établissement analysé
  - périmètre retenu
  - finesse de l'analyse de risques produite
  - détail de la PSSI

Synthèse : les comités SSI

Comité de pilotage stratégique	• Valide et gère la PSSI • 1 réunion par an (préconisation générique)
Comité de sécurité opérationnel	• Évolution de la PSSI, analyse et traitement des risques, processus de suivi • 3 à 4 réunions par an (préconisation générique)
Comité de liaison	• Relais des décisions de sécurité vers les composantes, gestion des incidents • Réunions régulières

Il est souvent plus simple d'affecter ces rôles à des comités déjà existants

Les livrables du projet

- La PSSI propre à chaque établissement
  accompagnée des documents d'étapes (analyse de risques)
- Le référentiel générique :
  - Une politique de management de la sécurité de l'information (PMSI)
  - Une politique de sécurité des systèmes d'information (PSSI)
  - Une politique générale de la sécurité des systèmes d'information (PGSSI)
  - Une matrice de correspondance des règles et mesures
  - Une déclaration d'applicabilité type (mise en œuvre)
  - Un plan d'action type pour l'implémentation d'un système de management de la sécurité de l'information (SMSI)

Focus sur 3 établissements

- Une université : l'Université de Rennes 1
- Un Pôle de Recherche et d'Enseignement Supérieur : le PRES Université de Grenoble (4 universités, 1 école d'ingénieurs et 1 institut d'études politiques)
- Une Université Numérique en Région : l'UNR RUNN - Réseau Universitaire Numérique Normand (3 universités et 2 écoles d'ingénieurs)

Organisation projet

Équipe projets		
	Composition	**Effectifs**
Rennes	RSSI, RSSI adjoint , responsable de cellule de proximité, un CSSI CNRS + l'animateur du groupe projet national	5
Grenoble	4 RSSI (ou adjoints) issus de 4 des 6 établissements du PRES	4
RUNN	4 personnes du groupe de travail SSI du RUNN (RSSI et animateur du groupe de travail)	4

La décision de participer au projet PSSI générique a été prise à un niveau politique dans les trois établissements.

Organisation projet (2)

Comité de pilotage projet			
	Comité existant	Composition	Effectif
Rennes	oui	Président, plusieurs Vice-Présidents, la Directrice Générale des Services, le Directeur du CRI, le RSSI	9
Grenoble	oui	Les DGS et les VP SI des 6 établissements, le Directeur du PRES, les 2 coordinateurs SSI inter-universitaire et le CIL	15
RUNN	non	2 VP et le chef de projet RUNN, les 5 DGS, un DSI, un ingénieur Hygiène et Sécurité, un CIL, un représentant du CNRS et l'équipe projet	16

Les entretiens

	Nombre	Durée totale
Rennes	25	1,5 mois
Grenoble	24	2 mois
RUNN	28 + 11	2 mois

Personnes interviewées

- DGS, VP
- Chefs de services ou responsables métiers (RH, Scolarité, Finances, H&S...)
- Directeurs d'UFR, IUT, Laboratoires...
- RSSI, DSI
- Informaticiens
- Responsables projets

Traitement des livrables

- La PMSI
  - Document organisationnel et stratégique
  - Adapté aux structures en place dans les 3 cas
- La PSSI de Rennes, 3 volets
  - PSSI - Principes généraux : issu de la PGSSI générique
  - PSSI - Règles : toutes les règles ont été révisées par un comité d'experts selon les domaines abordés
  - PSSI - Documents d'application : devra contenir tous les documents auxquels il est fait référence dans les règles

Traitement des livrables (2)

- La PSSI de Grenoble
  - La PGSSI est retenue comme PSSI. Nous restons ici à un niveau d'intention décliné suivant les règles ISO 27002 pour la politique, les règles précises mises en œuvre étant décrites dans des documents annexes.
  - La PSSI détaillée sert de base à la rédaction des documents annexes et à la mise en œuvre des mesures.

Traitement des livrables (3)

- La PMSI du RUNN
  - document organisationnel et stratégique définissant un cadre commun pour gérer la SSI dans les 5 établissements
- La PSSI du RUNN
  - document décrivant des mesures et des règles opérationnelles de sécurité applicables aux projets communs (PSSI générique adaptée au contexte local)
  - certaines règles font référence à des procédures et documents d'application plus détaillés (en cours d'écriture)

Les différents comités SSI

Comité de pilotage stratégique			
	Comité existant	Composition	Effectif
Rennes	oui	le comité stratégique du SI : Président, DGS, VP finance, 2 VP, DSI	6
Grenoble	variable suivant étab.	Pilotage stratégique du domaine de chaque établissement. Pour le périmètre recherche il existe un comité de coordination SSI Universités-CNRS	variable 15
RUNN	non	Pour chaque établissement : Président ou directeur, 1 personne désignée (FSD, DGS ou DSI), le RSSI + le chef de projet RUNN + un représentant du CNRS	17

Les différents comités SSI

Comité de sécurité opérationnel			
	Comité existant	Composition	Effectif
Rennes	non	RSSI, RSSI adjoints, CIL, un représentant du service juridique, représentants de la DSI, experts invités	5 à 10
Grenoble	Oui concatenation de comités existants	Pour chaque établissement : DGS, VP SI, DSI et RSSI Directeur du PRES + Directeur service informatique mutualisé	25
RUNN	Oui (GT SSI RUNN)	Pour chaque établissement : RSSI et RSSI adjoints RSSI régional du CNRS 1 assistant du groupe de travail	17

Les différents comités SSI

Comité de liaison			
	Comité existant	Composition	Effectif
Rennes	non	Pourrait être composé des chargés de la SSI dans les composantes et unités de recherche	31
Grenoble	oui	6 RSSI ou adjoints des établissements	6
RUNN	non	Comité de liaison au niveau de chaque établissement ex : pour l'Université de Caen comité de liaison composé des chargés de la SSI dans les composantes et unités de recherche (36 nommés à ce jour)	

Plans d'action

- En fonction des établissements des plans d'actions adaptés à la problématique locale sont en déploiement
- Points clés :
  - Appropriation de la PSSI au niveau de l'établissement
  - Sensibilisation de l'ensemble des acteurs, à tous les niveaux
  - Rédaction de documents d'application en impliquant les experts métiers

Difficultés rencontrées

- Le contexte et le périmètre
  - Difficiles à définir ou à appréhender
- L'analyse de risque
  - Le périmètre d'une Université est vaste, on ne peut pas descendre à un niveau trop fin dans l'analyse sous peine de se noyer dans l'étendue des données
  - Trouver un juste milieu n'est pas simple
- La charge de travail
  - L'équipe projet ne doit pas être trop réduite

Les apports

- La mise en place d'une gestion de la SSI, avec prise en compte des besoins, qui contribue :
  - à la maîtrise du SI
  - à la stratégie globale de l'établissement en matière de SI et de numérique
  - à l'image de marque de l'établissement
  - à un meilleur service rendu aux utilisateurs
- Un document listant de manière exhaustive tous les sujets de sécurité
- Prise de conscience des risques et des responsabilités de chacun

Conclusion

- Une PSSI pour une Université et même pour un PRES est possible !
- Tâche ardue mais faisable avec une organisation adaptée et un soutien de la gouvernance (1 équipe projet + 1 pilotage)
- Importance du contexte ; les entretiens sont un moment privilégié de sensibilisation
- Le pragmatisme est de mise !