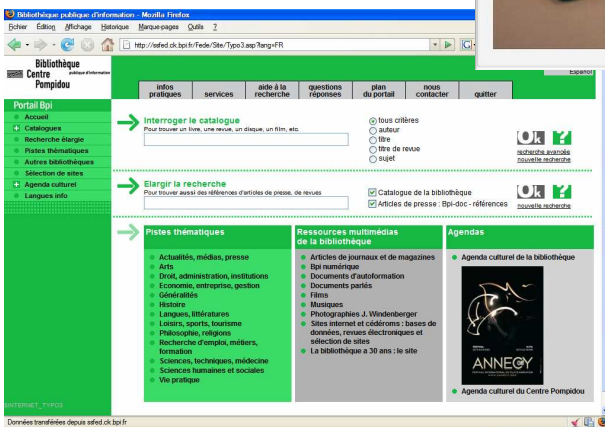
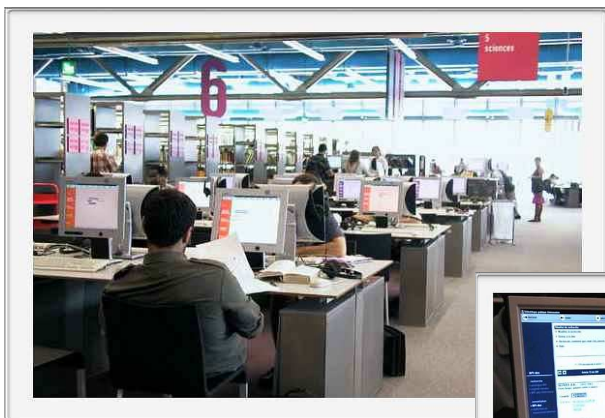


---

**Retour d'expérience**  
**Clusif**  
**4 décembre 2008**

---

Laurent Hugou – BPI  
Paul Grassart – Ageris Consulting



- Une des principales bibliothèques publiques parisiennes

- 400 000 documents, dont 352 000 volumes.
- Plus de 5000 visiteurs quotidiens
- 2200 places assises
- 450 postes publics, 250 postes professionnels, 70 serveurs
- 58 postes Internet en libre accès
- 241 permanents + 40 ETP de vacances

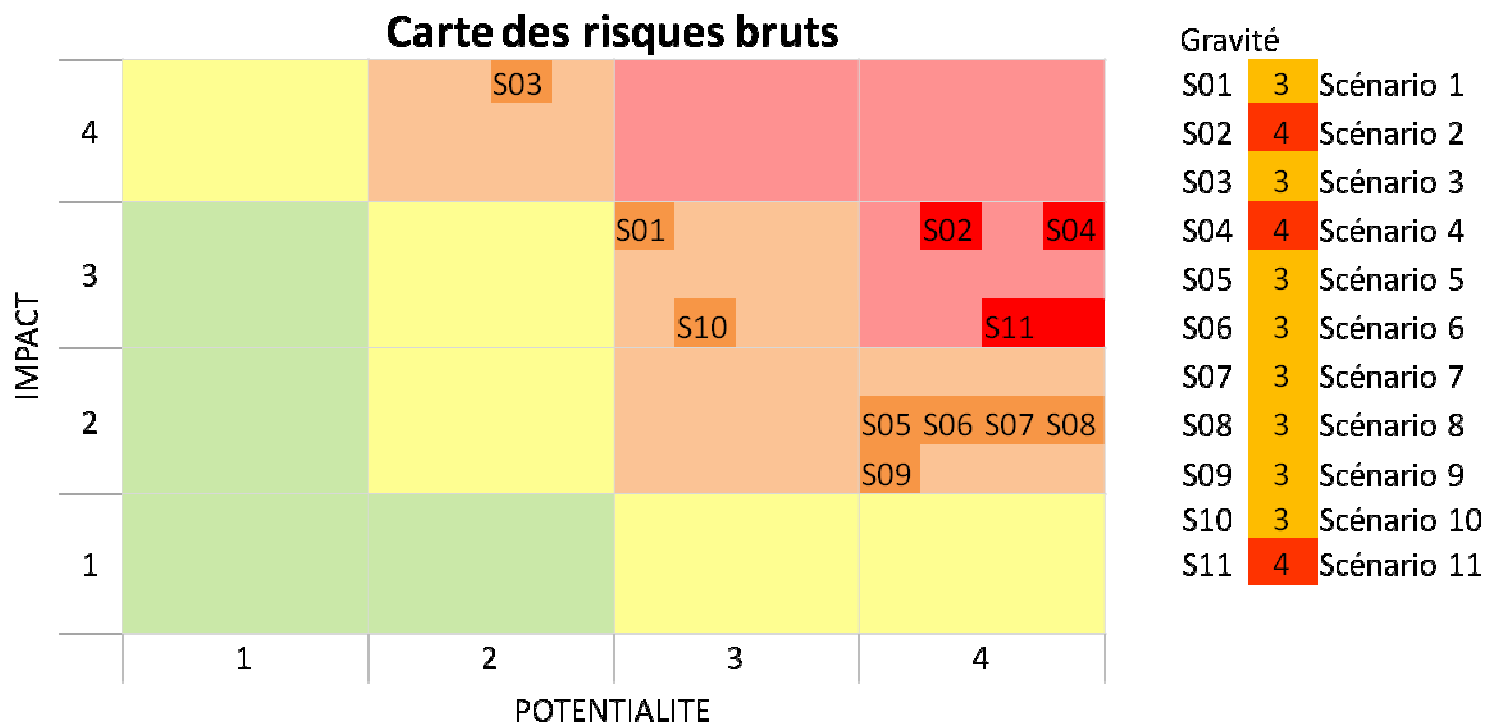
- Des services accessibles par Internet :

- Site web : consultation du catalogue, programme des animations, consultation des articles de presse, bibliographies... )
- Accueil dématérialisé du public : dialogue par chat ou par e-mail
- Gestion d'une base de 1800 signets de sites web
- Hébergement de colloques virtuels...

## Auditer la sécurité et proposer un plan d'actions

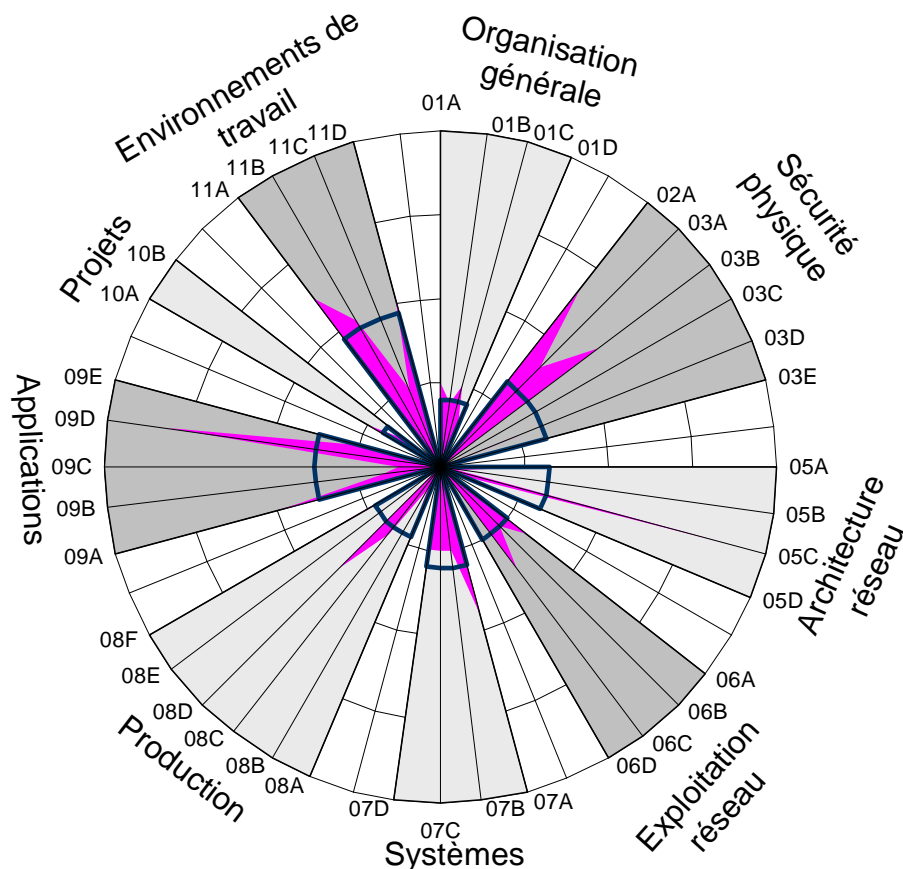
- **Identifier les vulnérabilités** organisationnelles et techniques (sur les plans physiques et logiques) pouvant avoir des conséquences graves sur les activités de la BPI
- **Évaluer la robustesse du système d'information** de la BPI sur le plan de la sécurité (notion de défense en profondeur pour la protection de ses ressources critiques)
- Cartographier différents **scénarios de risque** pertinents
- Proposer un **plan d'action** permettant de maintenir un niveau de risque acceptable, argumenté et organisé par priorités

- Un métier : mettre à disposition du public des informations, et ce de manière anonyme...



- Constat inquiétant :

**Peu de « bonnes pratiques » de sécurité mises en œuvre**



0 : non mis en œuvre

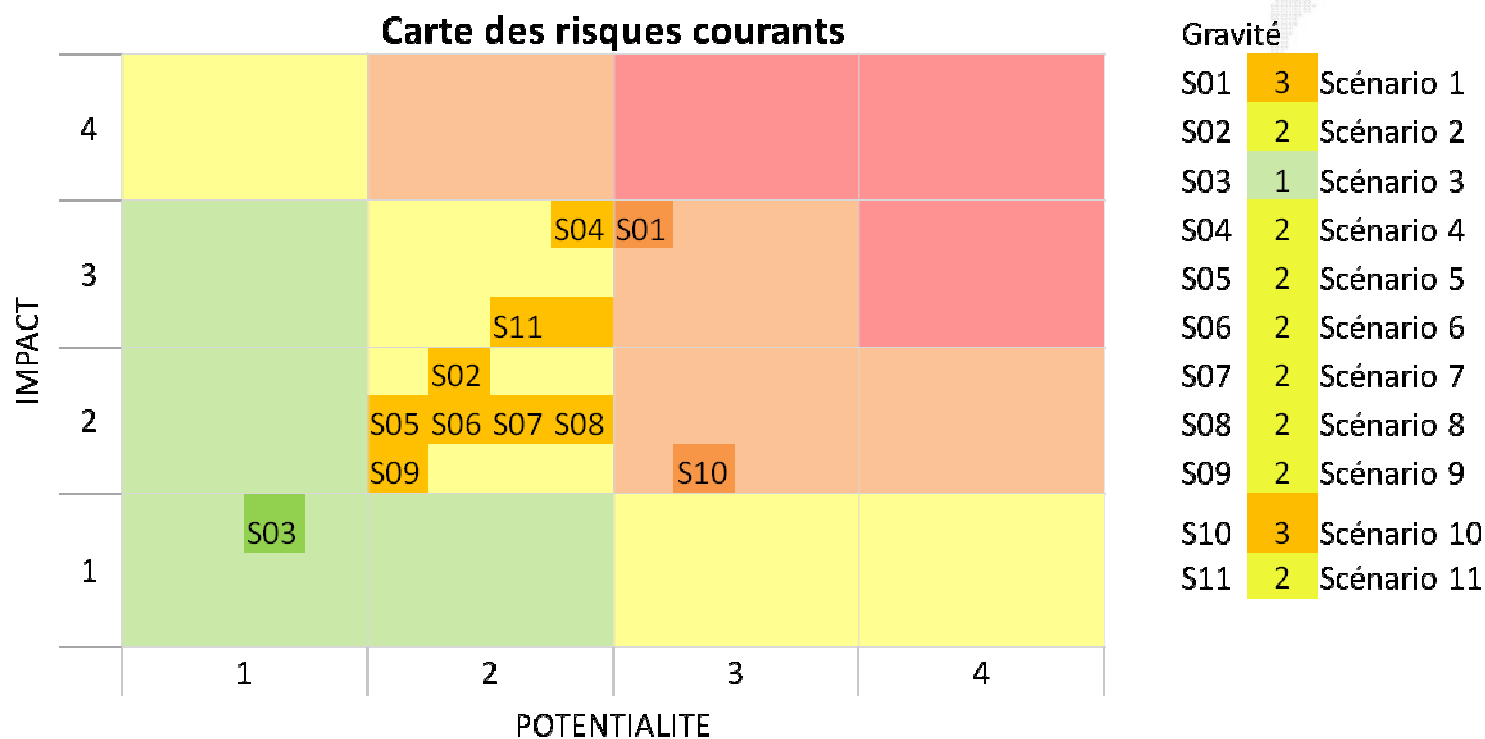
1 : mise en œuvre très partielle

2 : mise en œuvre partielle

3 : mise en œuvre et maîtrise

4 : pratique formalisée et sous contrôle

**Le constat ne serait pas fondamentalement différent avec ISO27002**



**Les pratiques mises en œuvre sont efficaces, adaptées au besoin et au contexte, et économiquement efficaces**

### Pertinence du référentiel de conformité ?

Pas de référentiel conçu pour des environnements comme la BPI...

Retour à des référentiels sectoriels ?

ISO27002 : supposé s'appliquer à tous

ISO27012 (?) Etablissements financiers

ISO27013 (?) Industrie manufacturière

ISO 27799 : Hôpitaux et santé

### La sécurité est un processus

Conformité : aide à la dynamique, et non objectif en soi

### Pertinence de la logique de conformité ?

Conformité : établir un socle commun **a minima**

(ex : PCIDSS)

L'analyse des risques revient au cœur de la gestion de la sécurité

Interprétation de l'ISO27001 très différente depuis la publication de ISO27005