

# METHODOLOGIE D'ANALYSE DES SYSTEMES D'INFORMATION



INSTITUT NATIONAL  
DES SCIENCES  
APPLIQUÉES  
CENTRE VAL DE LOIRE

# TD : Analyse de risques

- Sujet TD1:
  - Réaliser une analyse de risques sur un projet
  
- Consignes :
  - Faire une analyse de risques rapide sur papier libre
  - Définir les besoins de sécurité
  - Identifier les risques
  - Qualifier les risques



Microsoft Word  
Document

## Prenons le premier exemple

Objectif	Fournir un accès Internet à un pays		
Composants nécessaires	<ul style="list-style-type: none"> <li>Fibre</li> <li>Routeur</li> <li>PC</li> </ul>	<ul style="list-style-type: none"> <li>Câble Ethernet</li> <li>Ingénieur réseau</li> <li>Batiment</li> </ul>	
Les besoins	<ul style="list-style-type: none"> <li>Accès Internet tout le temps</li> <li>Accès Internet pour tout le monde</li> <li>Confidentialité des échanges</li> <li>Suivi des accès à Internet et de la maintenance</li> </ul>		
Les risques	Description	Impact	Probabilité
	Coupure d'Internet car fibre HS	Très fort	Faible
	Coupure d'Internet car routeur HS par une attaque physique (femme de ménage par exemple)	Moyen	Haute
	Coupure d'Internet car routeur HS par une attaque logicielle (remote access pour installer un APT dans le firmware)	Fort	Moyenne
	...		

# TD : Analyse de risques

## ■ Sujet TD234:

### ■ Créer un outil permettant de réaliser des analyses de risques SSI

## ■ Consignes :

- Faire un document autoporteur (inclure le contexte projet), préférer Excel comme support
- Pouvoir définir les besoins métiers
- Identifier les risques
- Evaluer les risques
- Déterminer les mesures de sécurité
- Avoir un plan d'action priorise
  
- Vous pouvez vous baser sur une méthodologie présentée en cours ou autre, ou proposer votre propre méthodologie en justifiant vos choix.
  
- A réaliser en groupe (4 personnes max)
- 3 points sur le partiel
- Soumission pour Vendredi 7/12 23h

# ANNEXES / EXEMPLES



New Risk (1)

1 Submit Risk

2 Plan Mitigation

3 Perform Reviews

4 Plan Projects

5 Review Regularly

Subject:

Category:

Site/Location:

External Reference ID:

Control Regulation:

Control Number:

Affected Assets:

Technology:

Team:

Additional Stakeholders:

Owner:

Owner's Manager:

Risk Source:

Risk Scoring Method:

Current Likelihood:

Current Impact:

Risk Assessment:

Additional Notes:

Supporting Documentation

Choose File

0 File Added

Max 1 Mb

Complete the form above to document a risk for consideration in Risk Management Process

Clear Form

Submit Risk

1 Submit Risk

2 Plan Mitigation

3 Perform Reviews

4 Plan Projects

5 Review Regularly

Inherent Risk

10

Very High

Residual Risk

5

Medium

ID #: 5254

Status: Mitigation Planned

Actions

Subject : Security Thing

## ▼ Hide Risk Scoring Details

## Classic Risk Scoring

Update Classic Score

Risk Scoring Actions

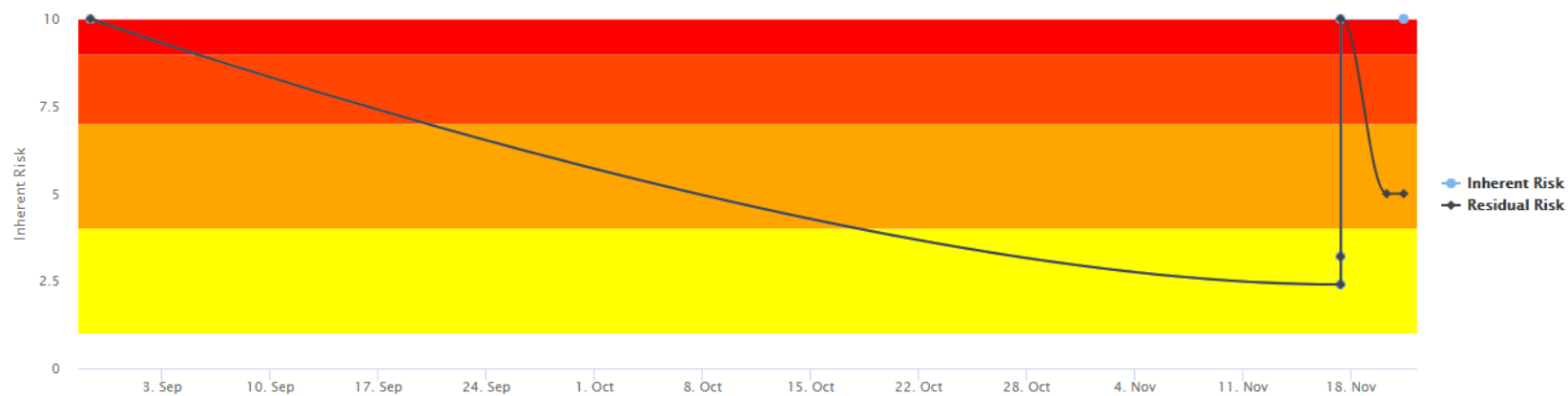
Likelihood: [ 5 ] Almost Certain

Impact: [ 5 ] Extreme/Catastrophic

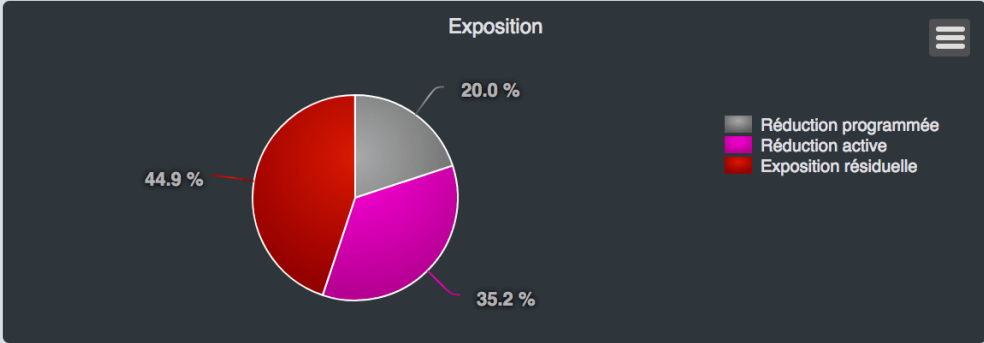
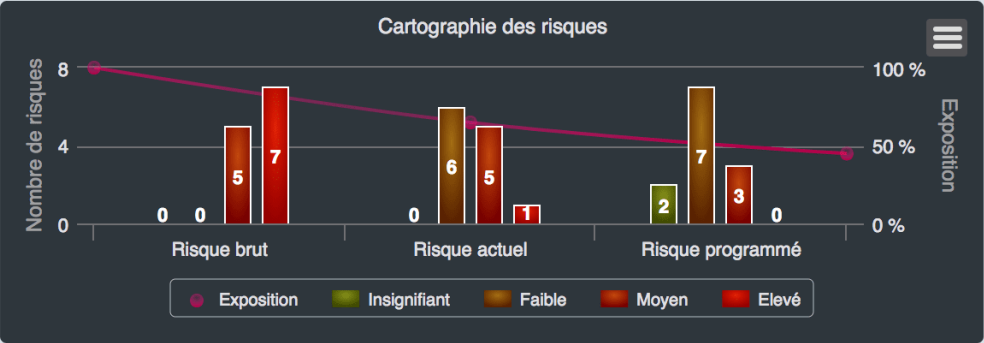
$$\text{RISK} = (\text{Likelihood} \times \text{Impact}) \times (10 / 25) = 10$$

## ▼ Hide Risk Score Over Time

Risk Scoring History



Scénarios de risques



Scénarios actifs 19 Scénarios inactifs 0 Événements redoutés PTR

+ Ajouter un scénario de risque

Action

Exporter

Filtrer

Rechercher...

7 champs affichés

Tout

		Brut	Actuel	Programmé	Exposition résiduelle	Intitulé	Propriétaire	État du traitement
<input type="checkbox"/>	Action	3.0	3.0	3.0	6.48 %	Une personne ayant un poste critique est absente, cette indisponibilité induit des dégradations de certains services essentiels		A traiter
<input type="checkbox"/>	Action	4.0	3.0	3.0	4.81 %	Une attaque par déni de service sur l'application ou sur le serveur rend indisponibles certains services essentiels		A traiter
<input type="checkbox"/>	Action	4.0	2.7	2.7	6.11 %	Un personnel de maintenance ou un administrateur du serveur détruit par erreur des données sensibles		A traiter
<input type="checkbox"/>	Action	3.0	2.4	2.4	5.19 %	Une attaque depuis le réseau de l'entreprise conduit à une intrusion dans le SI		A traiter



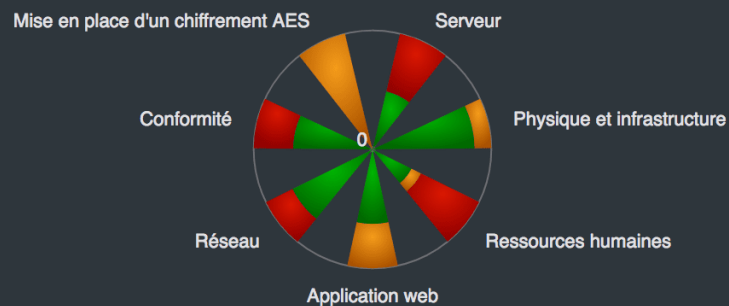
## Mesures

Bibliothèques

Historique

### Etat des lieux des mesures

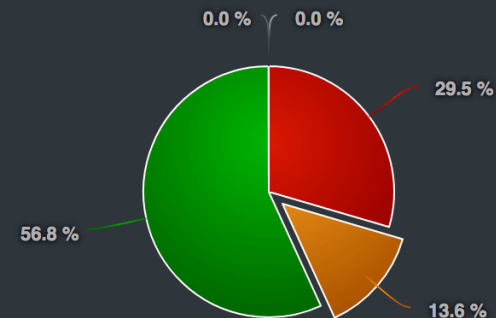
Source: EGERIE RiskManager



Non évaluée Non appliquée Programmée Appliquée Non applicable

### Implémentation des mesures

Source: EGERIE RiskManager



Non évaluée Non appliquée Programmée Appliquée Non applicable

Liste des mesures 56

Aide à la décision 44

PTR

+ Ajouter une mesure

Action

Exporter

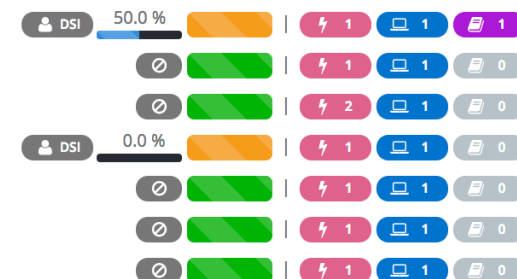
Filtrer

Tout déplier

Rechercher...



- ☐ Application web
  - ☐ Sécurité des applications
    - ☐ Application des mises à jour et des correctifs de sécurité sur l'application
    - ☐ Chiffrement des requêtes http (HTTPS)
    - ☐ Contrôle d'accès aux applications
    - ☐ Documentation des procédures d'exploitation des applications
    - ☐ Gestion et suivi des habilitations de l'application
    - ☐ Guide de bonnes pratiques de sécurité dans le développement
    - ☐ Journalisation des événements applicatifs



## Plan de traitement

6 Mesure(s) programmée(s) 💡

13.6 %



Coût total

14500 €



Charge totale

66 J/H



## Calendrier

octobre 2017						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				



■ Mesures programmées (date expirée)  
■ Mesures programmées (à venir)

## Plan de traitement

Exporter ▼

Rechercher...



9 champs affichés ▼

Tout ▼

Couverture (%)	Coût	Charge	Intitulé	Statut	Propriétaire	Personnes concernées	Scénarios de risques	Pourcentage d'avancement
7.8 %	2500	4	Procédure de validation des applications avant leur mise en production	<span style="background-color: orange; width: 100%;"></span>	DSI	1	2	0.0 %
6.6 %	2000	2	Application des mises à jour et des correctifs de sécurité sur l'application	<span style="background-color: orange; width: 100%;"></span>	DSI	1	2	50.0 %
5.6 %	0	20	Documentation des procédures d'exploitation des applications	<span style="background-color: orange; width: 100%;"></span>	DSI	1	1	0.0 %