


L'analyse de risques

François Thill
Manuel Silvano

 SMILE – home of:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur

AGENDA

Analyse de risques: Quoi et comment?

Étude de cas


Conclusions et perspectives

Rappelez-vous

**Chaque société dispose
d'informations critiques**

Rappelez-vous

Sécurité de l'information =
20% savoir-faire technique
80% organisation & comportement.

A young man with short dark hair, wearing a necklace, is smiling broadly and waving his right hand while underwater. Behind him, a large shark is swimming, its head and eyes visible. The scene is set in clear blue water.

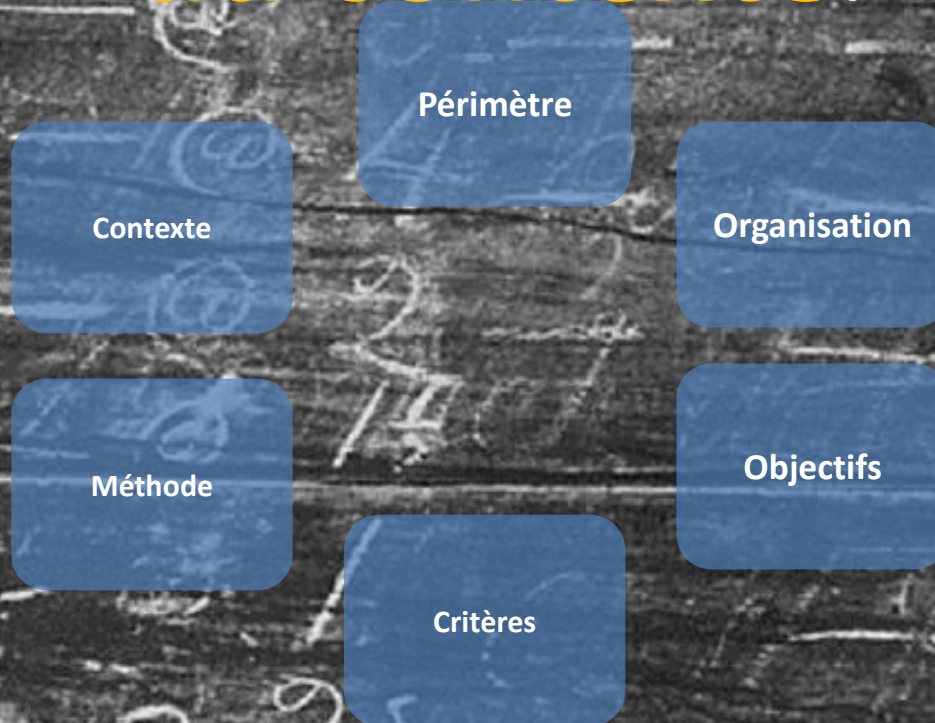
**Comment vous
comportez-vous?
Qu'en est-il de
l'analyse des risques...**

The background is a blue-tinted image of a document with handwritten text. Visible names include Philip 5, William 6, Stephen 7, and Charles 9. There are also some circled symbols and other faint markings.

Analyse des risques

Établissement du contexte :

Établissement du contexte:



CONTEXTE :

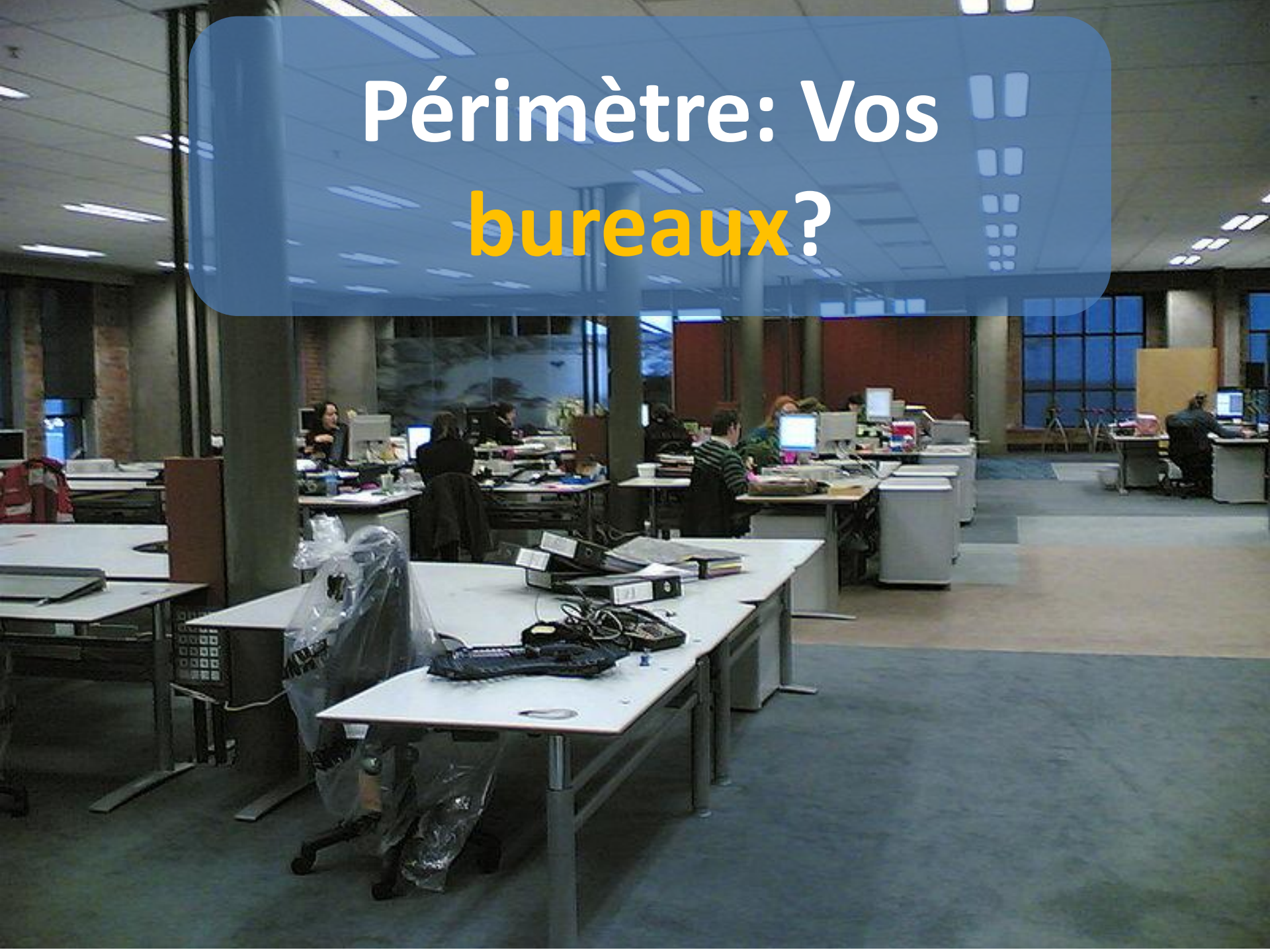
Confidentialité, intégrité ou
disponibilité?



Périmètre: Votre Informatique?

The National Archives (UK)

Périmètre: Vos bureaux?



Périmètre: Votre entreprise?



Effectifs: vos **experts**?



Méthode: **Reproductible?**



Critères: **Clairs?**

DATES	LECTURES	JAUGE G1. N°
15/11/94	0	



Etro
test Sintco
N.P.
78290 CR
14 111 35 14 7
6/8 rue Devallon
Y SUR SEINE - FRANCE
14 111 35 14 7

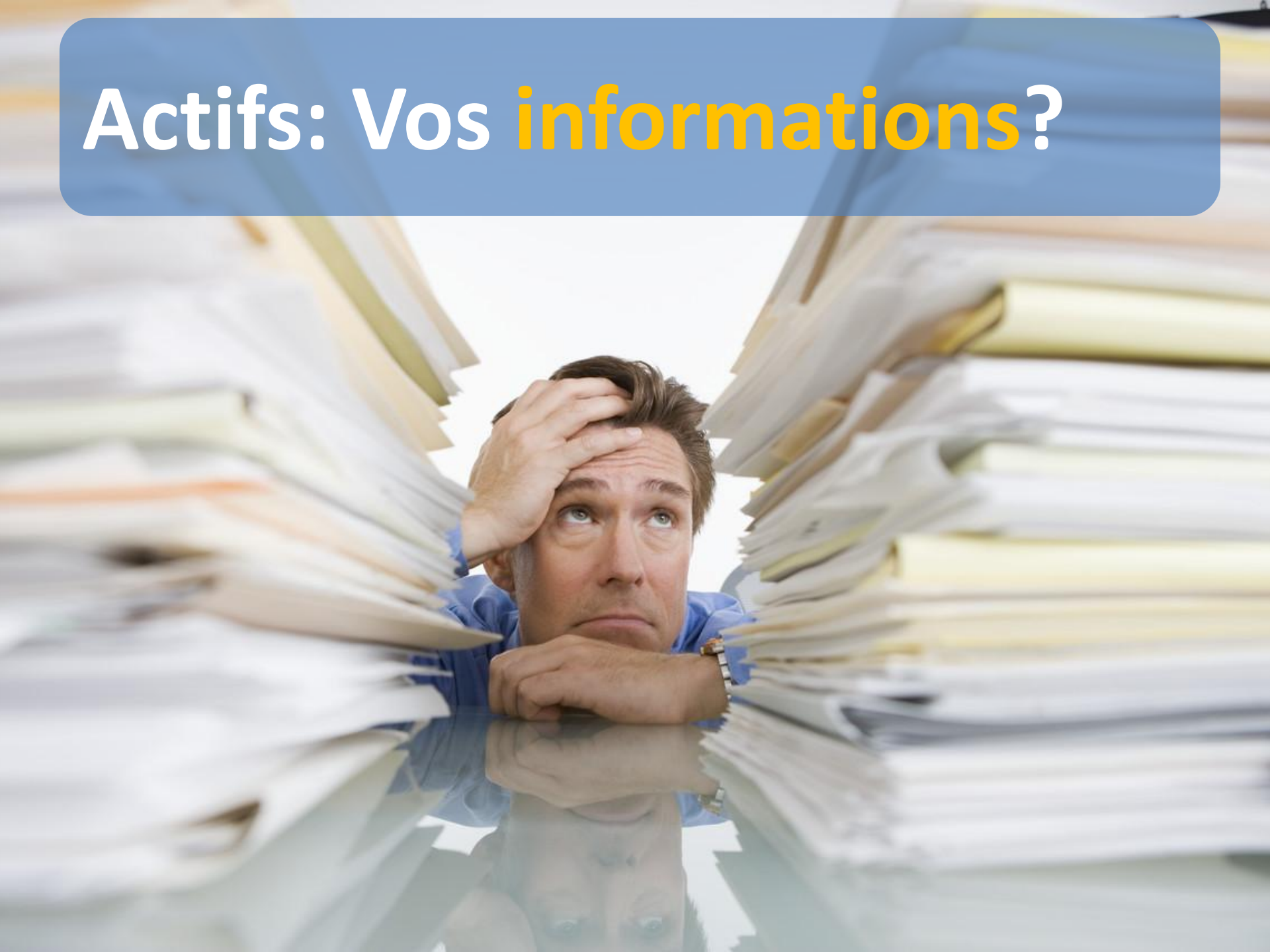
Objectifs: **Clairs?**



Appréciation du risque:

Les actifs :

Actifs: Vos **informations**?



Actifs: Votre **personnel**
et vos **machines**?



Actifs: vos **processus**?



Processus et actifs:
connaissez-vous les
dépendances?



Analyse des risques

D'autre part:

MENACES

MENACES: Environnementales ?



MENACES: Accidentelles?

CAUTION
THIS MACHINE
HAS NO BRAIN
USE YOUR OWN



Menaces: **Deliberées?**



Menaces: Probabilité?

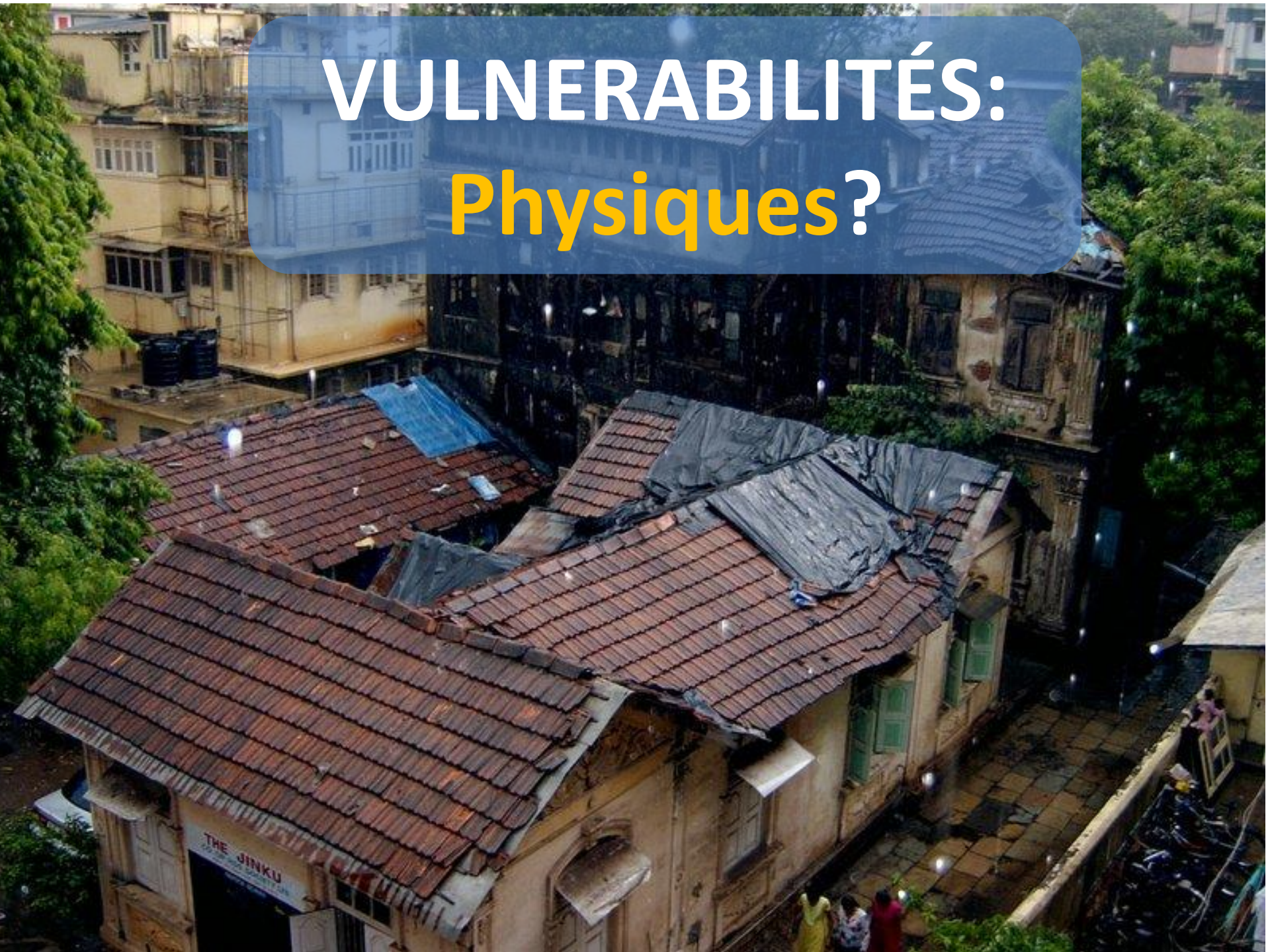


Analyse des risques

D'autre part:

VULNERABILITÉS

VULNERABILITÉS: Physiques?



VULNERABILITÉS: Classification?



VULNERABILITÉS: Organisationelles?



Comment peuvent-ils
facilement être
exploitées?



CONTEXTE - PÉRIMÈTRE - ACTIFS:

SONT TANGIBLES

MENACES ET VULNERABILITIÉS:

CHANGENT CONSTAMMENT

**Comment gérez-vous
ces changements?**





...workshop!



An aerial photograph of a large, multi-story brick building, likely a school or university, with a central entrance and a courtyard. The building has a complex roof structure with multiple gables and dormers. The courtyard in front of the building is paved and features a central landscaped area with greenery. The surrounding area includes other buildings and trees.

L'Étude de cas: Un lycée.

Durée : 25'

1 – Questions sur l'analyse de risques (15')

Périmètre

Processus

Menaces

Vulnérabilités

2 – Temps nécessaire pour faire une AdR (10')



Périmètre de l'analyse des risques **Que faut-il inclure**

- 1) Administration
- 2) Salles de classe
- 3) Locaux spéciaux comme laboratoires
- 4) Local informatique
- 5) Accès Internet

2

Processus dans l'AdR:
Criticité
de 1 (bas) à 5 (haut)

- 1) Processus administratifs
- 2) Processus éducatifs
- 3) Processus liés aux examens

3

Menaces sur les actifs processus d'examen:
Probabilité
de 1 (bas) à 5 (haut)

- 1) Usurpation de droits
- 2) Espionnage à distance
- 3) Divulgaration

4

Vulnérabilités des actifs liés au processus d'examens:

Aisance d'exploitation
de 1 (bas) à 5 (haut)

- 1) Absence de procédure formelle d'enregistrement et de radiation
- 2) Architecture de réseau non sécurisée
- 3) Pas d'anti-virus installé ou anti-virus non à jour

5

Analyse de risques
ETP estimation

Estimation du temps nécessaire pour
faire l'analyse de risques

A lighthouse with a white base, a purple band, and a red top section stands on a rocky coastline. The sky is overcast and grey, and the ocean is dark blue with white waves crashing against the rocks in the foreground.

Conclusions et perspectives

- L'analyse de risque peut être très **subjective**
- Le management de la sécurité de l'information est **difficile**
- Le management de la sécurité de l'information est **épuisant**



Il faut collaborer

- La **description des processus et actifs**
- L'évaluation des **menaces**
- L'évaluation des **vulnérabilités**



Il faut collaborer pour:

- Améliorer l'efficacité
- Améliorer l'objectivité
- Améliorer les compétences et le savoir-faire
- Améliorer les bases communes



La majorité a déjà été fait par vos voisins

concentrer sur une partie de ses activités ou le management peut souhaiter procéder par étapes successives dans le déploiement du système.

Il faut cependant veiller à ne pas écarter du domaine des processus de support indispensables ou indissociables des activités couvertes par le SMSI (exemple : gestion des ressources humaines, gestion de l'IT, etc.). Ces choix d'exclusion doivent donc rester cohérents.

Tâches	1. Définir le domaine d'application du SMSI qui se doit de contenir : <ul style="list-style-type: none"> • Les caractéristiques de l'organisme. • Les descriptions de ses activités. • Le ou les emplacement(s) physique(s) de l'organisme. • Ses écrits principaux. • Les technologies utilisées. • Justification du périmètre choisi.
Entrées	Références sur l'activité de l'organisme: orientations stratégiques, enjeux de sécurité, organigramme, exigences client, lois et règlements applicables, normes sectorielles, etc.
Sorties	Domaine d'application contenant la liste des processus, la justification des exclusions, etc.
Acteurs	Direction, Responsable du SMSI

Entrées	Domaine d'application Organigramme de l'organisme Procédures, descriptions, listes, bonnes pratiques, orientations stratégiques existantes, etc.
Sorties	Compte rendu de bilan de l'existant
Acteurs	Direction, Management, Responsable du SMSI
Outils	Diagnostic 27001 (DIV-1)

2.5 Planification

En se basant sur le compte rendu de bilan de l'existant, il convient d'ordonner les tâches principales et de répartir les acteurs et les charges. Cette formalisation du travail permet aux membres de l'équipe projet de communiquer les tâches futures à la direction et à l'ensemble du personnel. De plus, le planning du projet constitue un outil essentiel de suivi et de management durant le déploiement du SMSI.

Tâches	1. Réaliser un planning d'implémentation en se basant sur les tâches et documents à produire identifiés lors du bilan de l'existant. 2. Identifier les grandes étapes, les subdiviser en tâches. Pour chacune des tâches définir : <ul style="list-style-type: none"> • Le détail des actions à réaliser. • Le responsable. • La durée estimée. • Les ressources impliquées. • Les dates de début et fin prévues.
---------------	---

Sorties	Planning de projet
Acteurs	Direction, Management, Responsable du SMSI
Modèle	Planning (DIV-2)

3 Déploiement

3.1 Politique du SMSI

La politique du SMSI définit l'orientation stratégique de la direction. Ce document reprend l'orientation générale, les contraintes réglementaires et la stratégie de gestion du risque en matière de sécurité de l'information.

Tâches	Rédiger la politique du SMSI en synthétisant sur quelques pages : <ol style="list-style-type: none"> 1. Les objectifs et orientations générales concernant la sécurité de l'information. 2. Les contraintes actuelles applicables (lois, réglementation, normes, standards, contraintes métier et environnementales) ainsi que les éventuelles déclarations d'intention de mise en conformité. Les obligations légales luxembourgeoises en matière de sécurité des systèmes d'information peuvent concerner notamment : <ul style="list-style-type: none"> • Le respect de la propriété intellectuelle et des droits d'auteurs (notamment la « loi du 18 avril 2001 sur les droits d'auteur » mais aussi le « règlement grand-ducal du 17 novembre 1997 » au sujet des brevets et la « loi du 16 mai 2006 portant approbation de la Convention Belux du 23 février 2005 en matière de propriété intellectuelle » pour les marques, dessins ou modèles). • La protection des données opérationnelles obligatoires et des données à caractère personnel (loi modifiée du 2 Août 2002). • Le respect de la législation sur le droit du travail (comme le traitement de données à caractère personnel à des fins de surveillance des salariés sur le lieu de travail « Art. L 261-1 » ou encore la gestion des clauses de non concurrence « Art. L 125-6 »).
---------------	--

2.4 Bilan de l'existant

La mise en place d'un SMSI commence par une analyse de l'écart entre l'état actuel de l'organisme et les exigences nécessaires pour atteindre les objectifs stratégiques de sécurité fixés. Cet état des lieux se limite au domaine d'application défini à l'étape précédente.

Le premier état des lieux porte sur le périmètre de l'organisme à évaluer et à modifier.



Arrêtz de réinventer

	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	ANALYSE DES RISQUES		Afficher les risques à traiter		Afficher les risques acceptés		Afficher tous les risques		Nettoyer tableau					
2														
3	ACTIF BUSINESS (PROCESSUS)	VALORISATION	MENACE	NIVEAU DE MENACE	CRITERE (S)	MAX(CRITERE(S) IMPACTE(S)	VULNERABILITES	NIVEAU DE VULNERABILITES	RISQUE	COMMENTAIRE	TRAITEMENT	MESURES (DdA)	NOUVEAU NIVEAU DE VULNERABILITE	RISQUE RESIDUE
5	Inscription des clients	3 3 3	Atteinte à la maintenabilité du système d'information	1	x	3	Intervention inadéquate du service de maintenance	2	6	Acceptation				
6	Inscription des clients	3 3 3	Atteinte à la maintenabilité du système d'information	1	x	3	Maintenance insuffisante/installation défectueuse de média de stockage	3	9	Transfert				
7	Gestion des commandes	2 1 3	Dysfonctionnement logiciel	2	x x	3	Logiciel immature ou nouveau	1	6	Acceptation				
8	Gestion des commandes	2 1 3	Dysfonctionnement logiciel	2	x x	3	Spécifications peu claires ou incomplètes pour les développeurs	2	9	Réduction	A.12.5.2, A.12.5.3, A.12.5.5		1	6
9	Gestion des commandes fournisseurs	2 3 2	Dysfonctionnement logiciel	2	x x	3	Logiciel immature ou nouveau	1	6	Acceptation				
10	Gestion des commandes fournisseurs	2 3 2	Dysfonctionnement logiciel	2	x x	3	Spécifications peu claires ou incomplètes pour les développeurs	2	9	Réduction	A.12.5.2, A.12.5.3, A.12.5.5		1	6
11	Expédition des commandes	0 1 2	Dysfonctionnement logiciel	2	x x	2	Logiciel immature ou nouveau	1	4	Acceptation				
12	Expédition des commandes	0 1 2	Dysfonctionnement logiciel	2	x x	2	Spécifications peu claires ou incomplètes pour les développeurs	2	6	Acceptation				
13	Gestion des fournisseurs	3 1 1	Dysfonctionnement logiciel	2	x x	1	Logiciel immature ou nouveau	1	2	Acceptation				
14	Gestion des fournisseurs	3 1 1	Dysfonctionnement logiciel	2	x x	1	Spécifications peu claires ou incomplètes pour les développeurs	2	3	Acceptation				
15	Passage de commande	3 3 3	Ecoute passive	1	x	3	Les mots de passe des clients peuvent être trop courts	3	9	Acceptation	A.11.3.1		1	3

Réutilisez:

- 1) Approches
- 2) Processus
- 3) Objets
- 4) Métriques



Concentrez-vous sur:

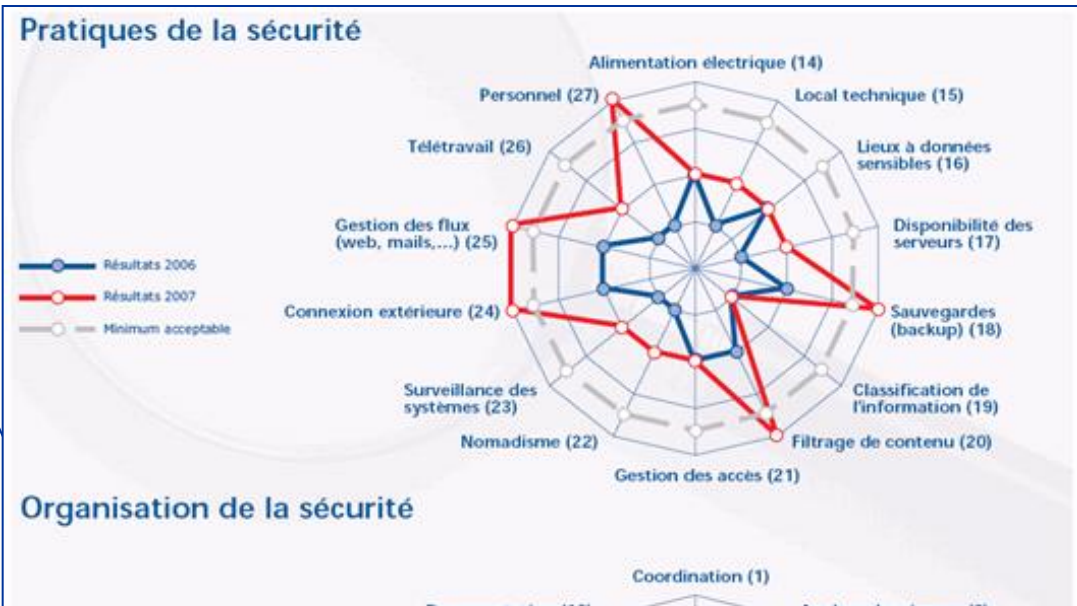
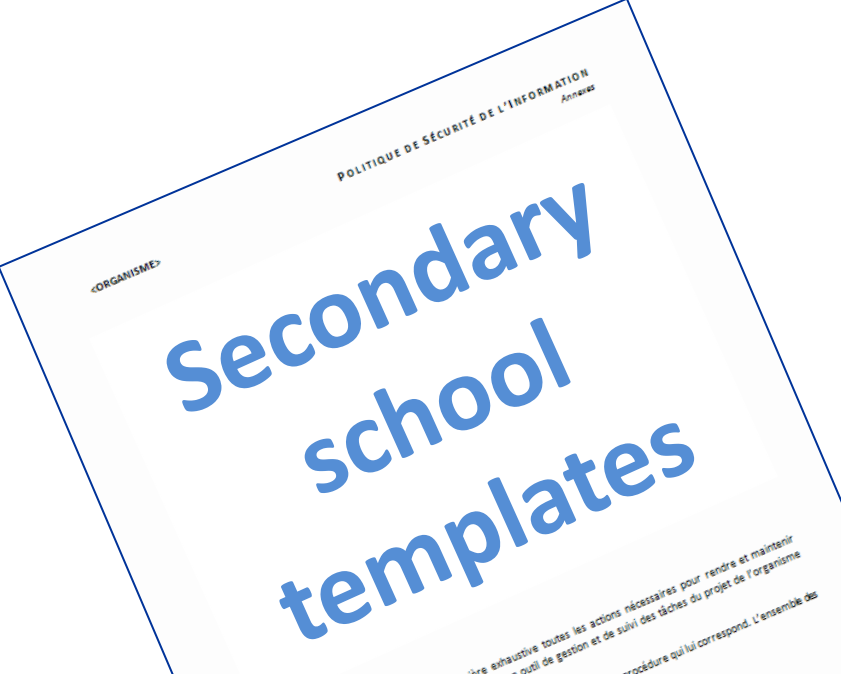
- 1) **Adaptation** vos spécificités
- 2) **Innovation**
- 3) **Sensibilisation** et formation





'SMILE' plate-forme:

- Offre outils et templates adaptés
- Échange d'expériences et de savoir-faire
- Promeut la confiance



Utilisez des outils simples et existants!

2					
3					
4					
5					
6		Procédure de gestion des incidents non critiques	13		Technique
7		Procédure de gestion des incidents critiques	13		Technique
8		Procédure de revue indépendante de la sécurité de	6		Organisationnel

A large crowd of people is shown in a dark setting, possibly a concert or protest. The lighting is dim, with a warm, reddish glow. In the foreground, a person is holding a lit candle, which is the primary light source for the scene. The crowd is dense, and many people are looking towards the camera or slightly to the side. The overall atmosphere is somber and collective.

Pourquoi agir comme si vous étiez
 toujours **seul**?




Ensemble, vers la cybersécurité!

Pour aller plus loin:

- https://www.cases.lu/pourquoi_gerer_les_risques.html
- https://www.cases.lu/pourquoi_mutualiser_l_analyse_des_risques.html
- <https://www.cases.lu/gestion-du-risque.html>

Merci beaucoup

francois.thill@eco.public.lu
manuel.silvoso@eco.etat.lu

 SMILE – home of:



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie
et du Commerce extérieur