

## Agenda

### OBJECTIF

### RISQUES

- Objectifs de contrôle

### CONCEPT GLOBAL

### PROCESSUS D'AUDIT

- Sécurité physique
- Discrétion du site
- Visiteurs
- Santé et sécurité
- Environnement
- Alimentation électrique

### Conclusion



Cours Audit des SI >> 16.11.2005

# Audit de la sécurité physique

**Cédric Gaspoz**

Assistant recherche et enseignement  
HEC Lausanne

*Unil*

UNIL | Université de Lausanne  
HEC Lausanne

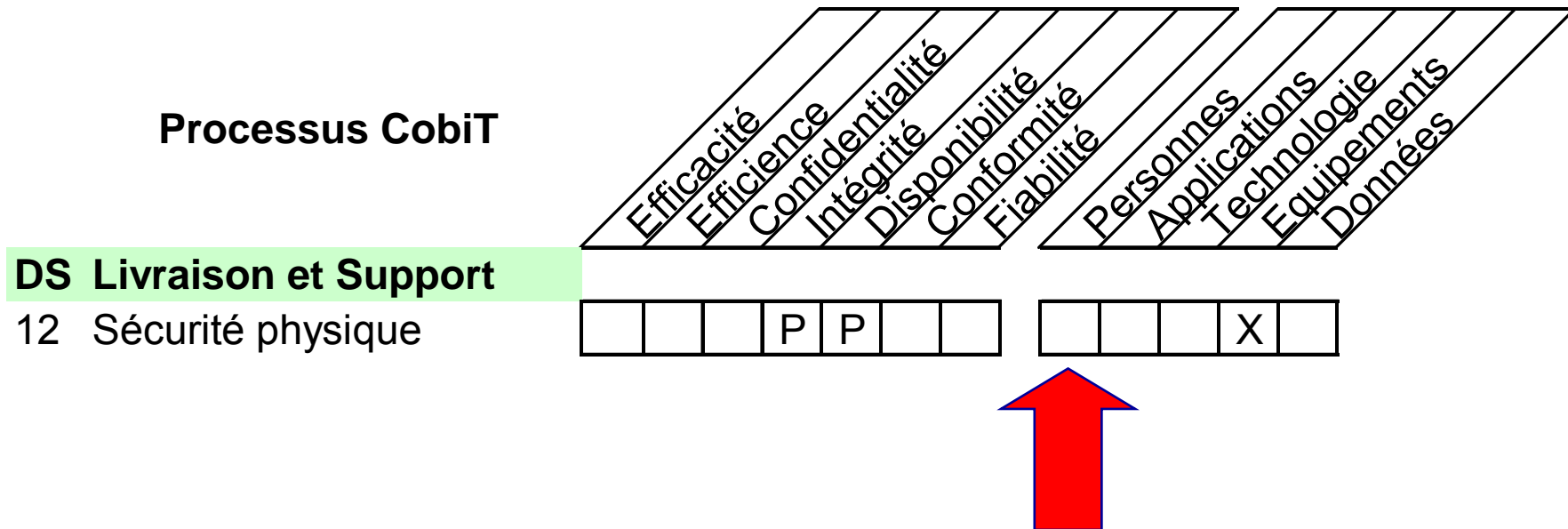
## Objectif

**Fournir un environnement physique adapté qui protège l'équipement informatique et les personnes contre les risques humains et naturels.**

- L'accès aux installations
- L'identification du site
- La sécurité physique
- Les politiques d'inspection et d'escalade
- Le plan de continuité des activités et la gestion de crise
- La santé et la sécurité du personnel
- Les politiques de maintenance préventive
- La protection contre les menaces de l'environnement
- La surveillance automatisée

# Risques

Les hommes sont essentiels pour la bonne marche des data centers. Toutefois les études montrent que les hommes sont responsables de **60% du downtime** des data centers à cause d'accidents et d'erreurs — procédures non respectées, équipements mal identifiés, objets ou liquides renversés, commandes mal entrées et autres erreurs plus ou moins importantes.

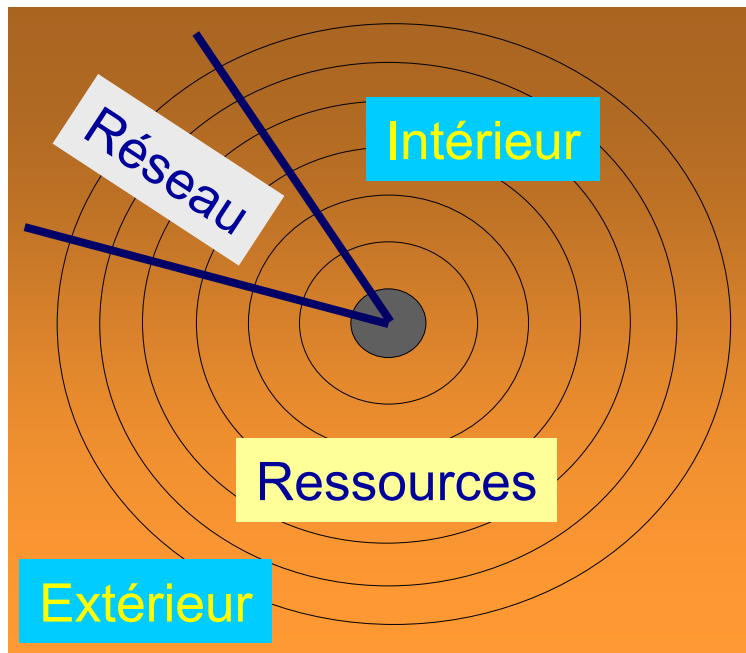


## Objectifs de contrôle du CobiT (DS12)

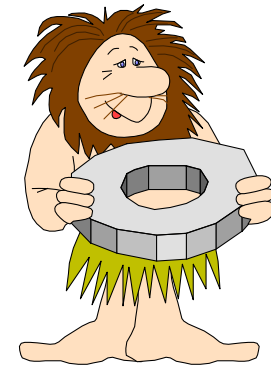
- 12.1 Sécurité physique
- 12.2 Discretion du site informatique
- 12.3 Accompagnement des visiteurs
- 12.4 Santé et sécurité du personnel
- 12.5 Protection contre les risques liés à l'environnement
- 12.6 Continuité de l'alimentation électrique

## Concept général

La sécurité physique est le premier rempart (après l'humain) pour assurer la protection des données de l'entreprise



- Données
- Programmes
- Applications
- OS
- Plates-formes
- **Bureaux, locaux,**
- **Immeubles, équipements**



## Processus d'audit

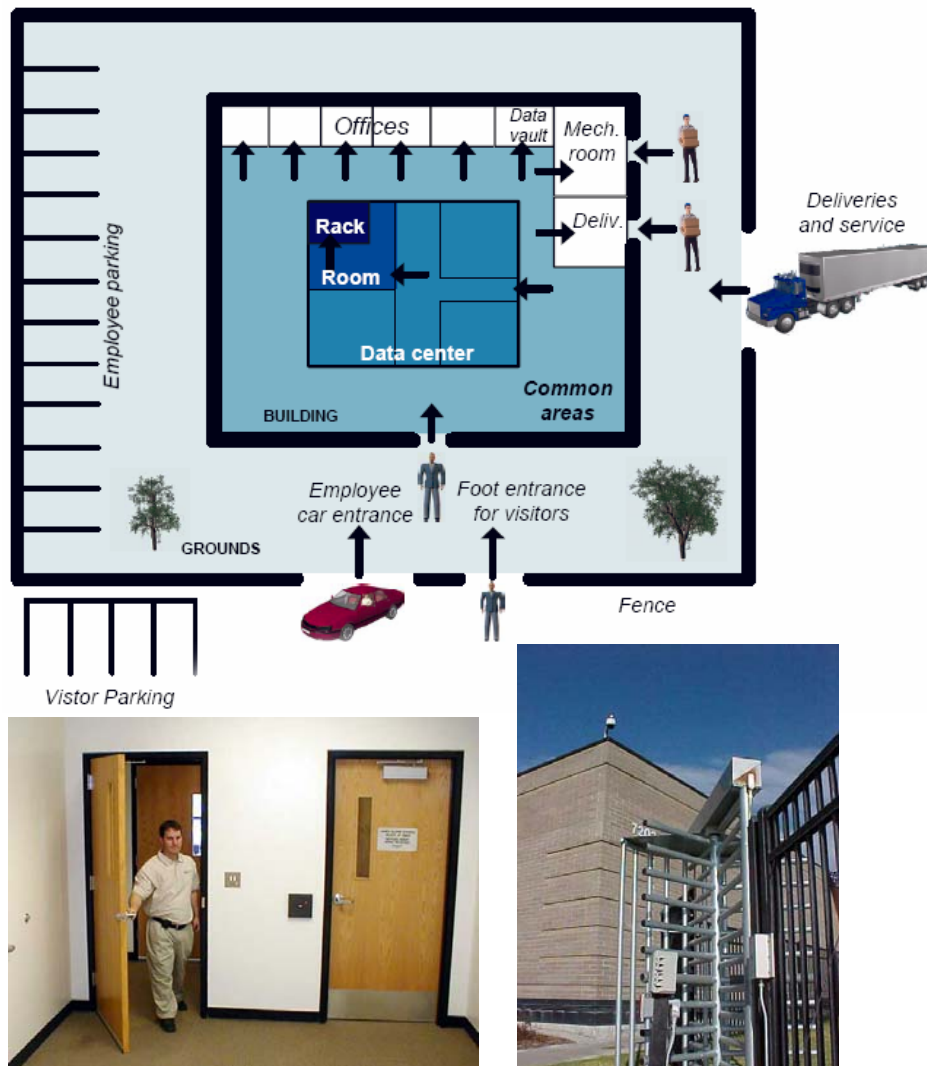
- La sécurité de tout l'ensemble sera toujours  $\leq$  à la sécurité du maillon le plus faible!
- La sécurité physique des SI doit être partie intégrante de la politique de sécurité globale de l'entreprise
- L'audit de la sécurité physique des SI se base en premier lieu sur la politique de sécurité définie par l'entreprise, son respect par le personnel, la formation de ce dernier ainsi que l'analyse des traces et des historiques

## 12.1 Sécurité physique

- Protéger le périmètre avec des clôtures de sécurité
- Entrée des véhicules des employés/livraisons surveillée par un gardien
- Parking visiteurs à l'extérieur du périmètre
- Protéger le bâtiment par des éléments naturels
- Limiter les points d'accès au minimum et les répartir en fonction des besoins des personnes
- Eviter les fenêtres, poser des vitres blindées
- Eviter les murs communs entre le data center et l'extérieur
- Poser des issues de secours à sens unique
- Protéger les équipements de secours s'ils sont à l'extérieur du centre de calcul
- Surveiller les sorties
- Utiliser des caméras de surveillance (LPD!)
- Mettre le data center sous alarme complète: feu, mouvement, paramètres env,...

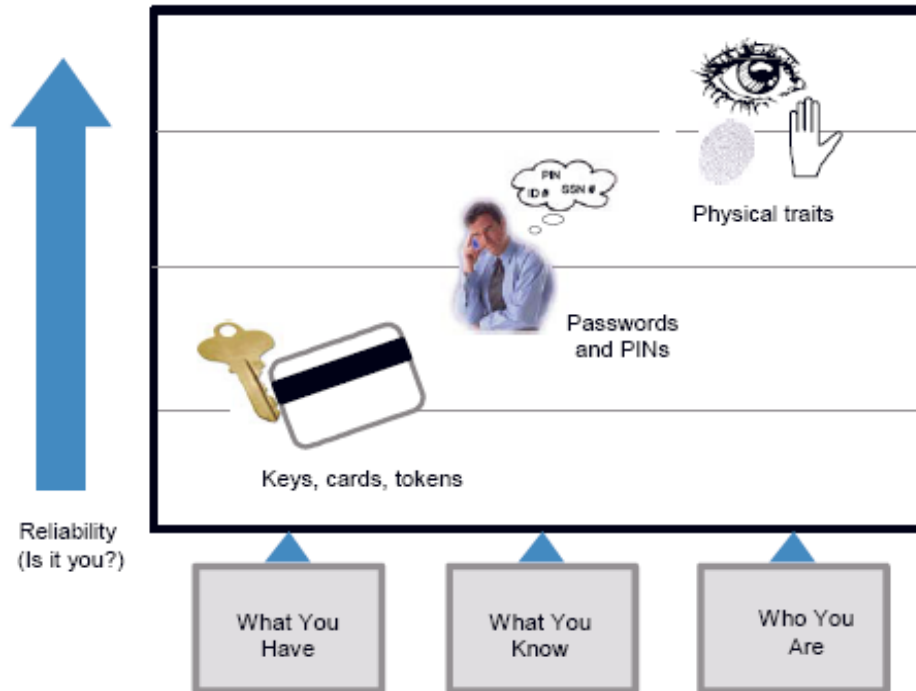


## 12.1 Sécurité physique (accès)



- Accès en fonction des besoins et non des personnes
- Former des périmètres concentriques (une personne est authentifiée N fois avant d'entrer dans le data center)
- Utiliser des badges sur les portes (mantrap), verrouiller les racks
- Garder des traces de tous les accès (positifs ou négatifs)
- Gestion restrictive des droits d'accès (one-time, échéance, ...)

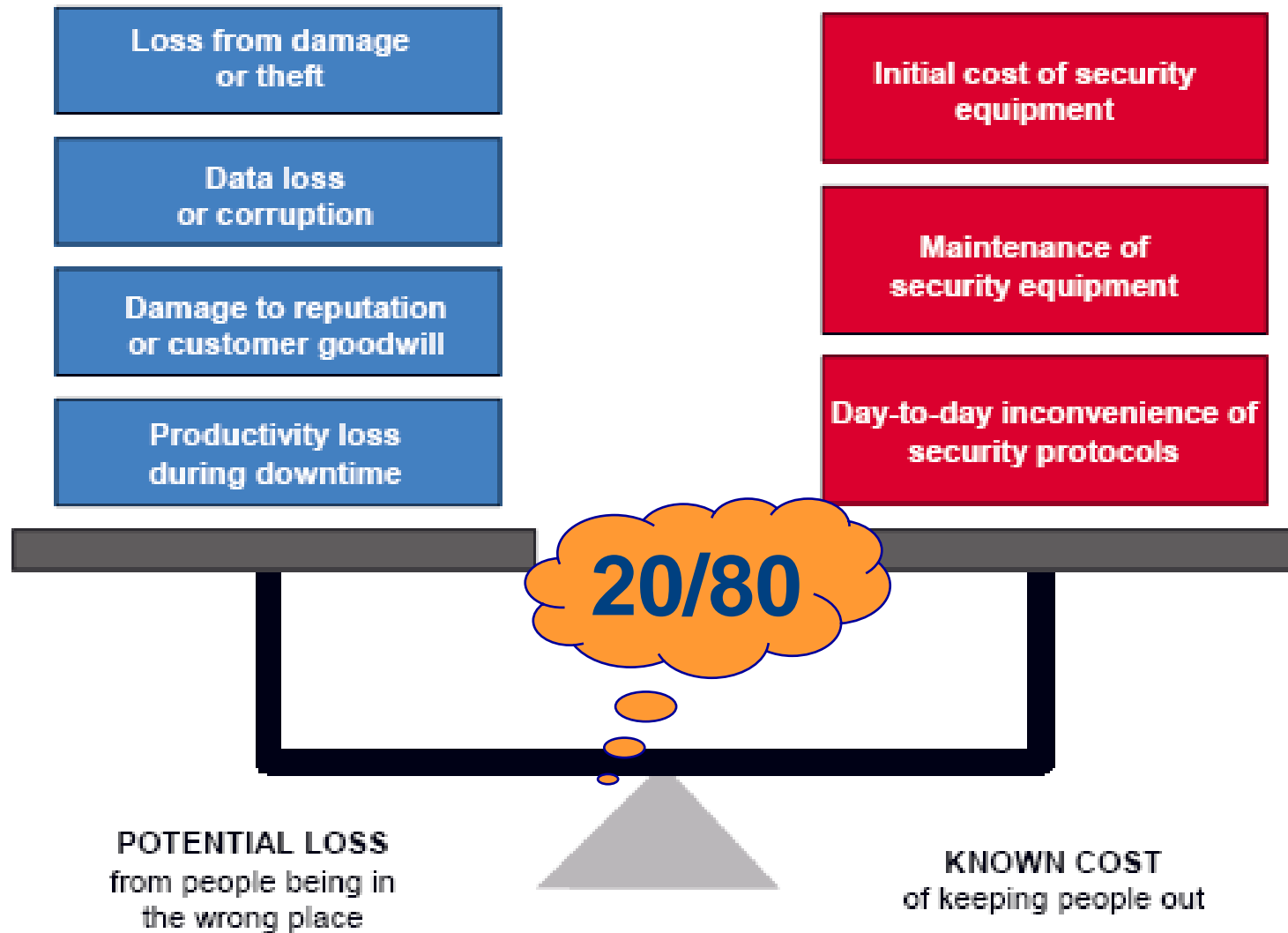
## 12.1 Sécurité physique (authentification)



- Authentification à deux facteurs
- Le gardien est toujours plus performant qu'un système automatique
- Empêcher le vol d'identité
- Panacher les systèmes



## 12.1 Sécurité physique (compromis)



## 12.2 Discrétion du site informatique

- Rendre le site totalement anonyme (ne pas l'identifier ou le rendre identifiable), si nécessaire utiliser un nom fantaisiste
- Si le site n'est pas dédié, mélanger les utilisations pour « noyer » le data center parmi les autres activités
- En cas de recours fréquents à des prestataires, prévoir des parkings à l'abri des regards



## 12.3 Accompagnement des visiteurs

- Etablir une politique d'accès globale comprenant toutes les exceptions
- Tous les utilisateurs du site doivent s'y soumettre
- Identifier clairement les visiteurs par un badge spécial à durée limitée
- Accompagner et raccompagner les visiteurs
- Installer des sanitaires/vestiaires pour les visiteurs
- Ne jamais laisser un visiteur seul se promener dans le bâtiment
- Tout visiteur doit avoir une autorisation d'accès délivrée par un responsable (maintenance, entretien, visites, réunions, ...)
- Concevoir le data center de façon à ce que la présence d'équipes de nettoyage ne soit pas nécessaire dans la salle des serveurs (meublement anti-statique, filtres à particules, ...)
- Ne pas placer le NOC avec les systèmes
- Séparer les accès



## 12.4 Santé et sécurité du personnel

- Eviter les possibilités de contrainte sur le personnel (vol d'identité, vol de matériel, ...)
- Utiliser des systèmes d'extinction neutres sur les humains
- Equiper le data center d'aspiration de fumée et/ou de respirateurs
- Placer l'éclairage, les systèmes de sécurité ainsi que les mécanismes d'ouverture des issues sur une alimentation sécurisée
- Marquer les issues de secours et les mesures à prendre en cas d'alarme
- Tester les scénarios en cas de faille de sécurité (intrusion, vol, ...)



## 12.5 Protection contre les risques liés à l'environnement

- Considérer les risques environnementaux (inondations, aéroport, avalanches, glissements de terrain, raffinerie, lignes haute-tension, gazoduc, tremblement de terre, ...) et prévoir des mesures de protection
- Considérer les risques externes ET internes (inondations, feu, ...)
- Construction résistante, normes anti-feu, ...
- Stocker les matières inflammables à l'extérieur des zones sensibles (cartons, emballages, manuels, ...)
- Tester les mesures régulièrement



## 12.6 Continuité de l'alimentation électrique

- Définir ce qui doit être placé sur l'alimentation de secours (systèmes, NOC, éclairage, senseurs, gestion accès, ...)
- Utiliser deux alimentations électriques provenant de deux sous-stations différentes géographiquement séparées
- Doubler tous les systèmes techniques (UPS, génératrices, climatisation)
- Tester l'alimentation électrique de secours mensuellement (générateurs et/ou batteries)
- Stocker suffisamment de carburant pour 24 heures et signer un contrat pour un approvisionnement immédiat en cas de besoin

