Ecole de Management Strasbourg

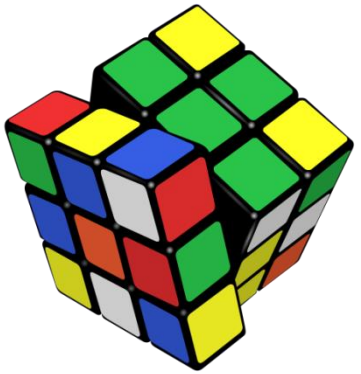
UNIVERSITÉ DE STRASBOURG

www.em-strasbourg.eu

Module 1: Introduction à la Sécurité des Systèmes d'Information

Octobre 2019

I) INTRODUCTION GENERALE



Définitions

- L'information est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.
- Sous forme électronique, l'information est traitée par le **système d'information (S.I.)** de l'organisation.

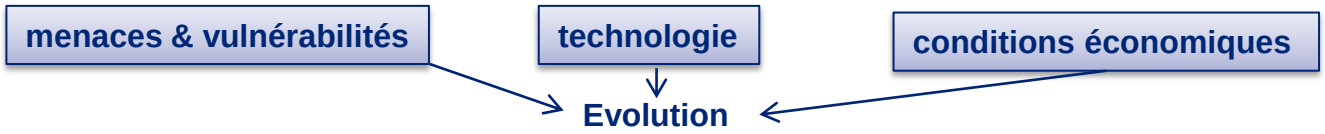
➢ **Système d'information (S.I.):**

Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser** les informations au sein d'une organisation.

Le S.I. doit permettre et faciliter la mission de l'organisation.

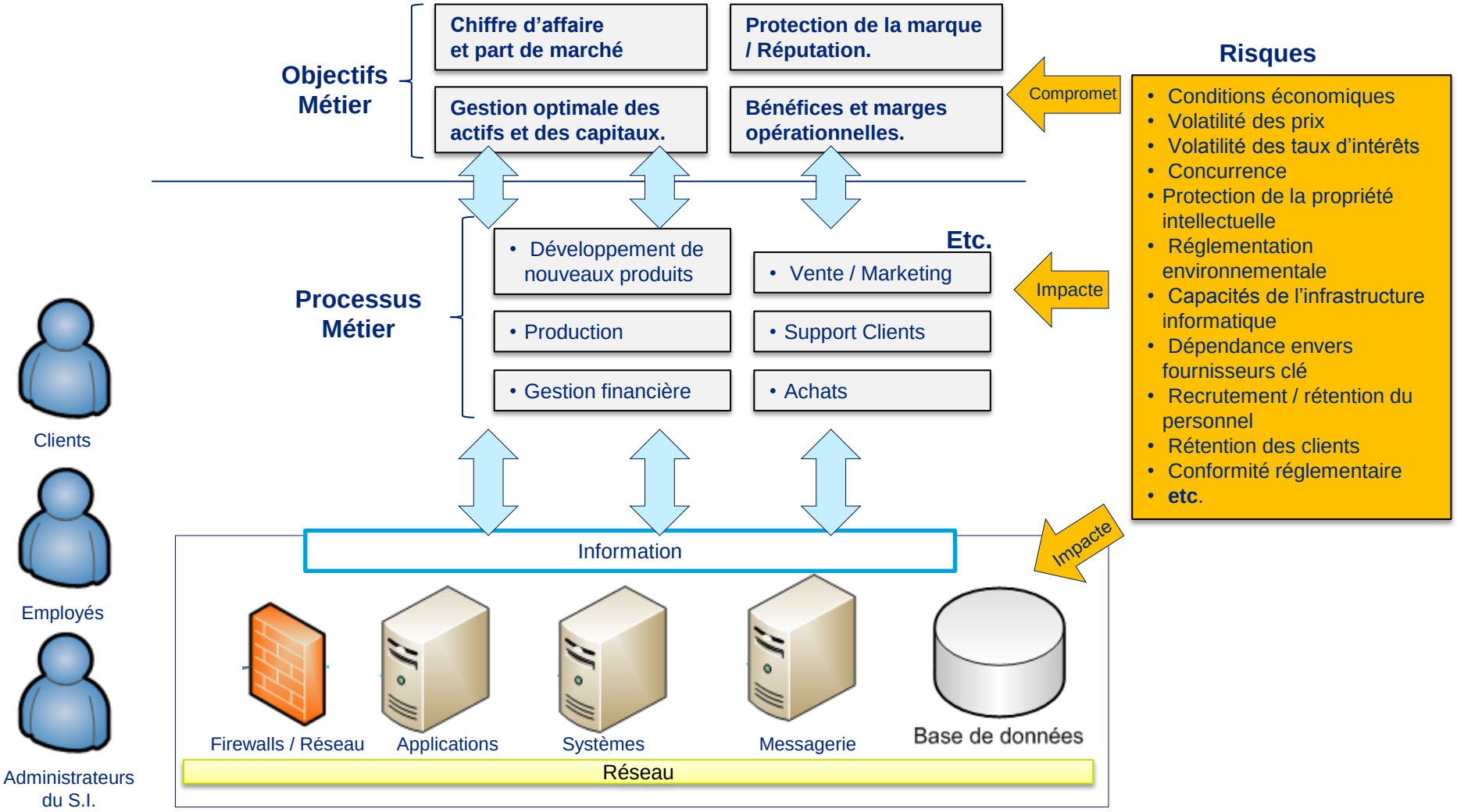
Le fonctionnement du S.I. doit être fiable et homogène dans le temps,

La fiabilité, un objectif difficile à atteindre. « Les systèmes informatiques ne sont pas naturellement sûrs » (Bruce Schneier)



Introduction à la Sécurité des Systèmes d'Information

Le rôle du Système d'Information dans l'entreprise

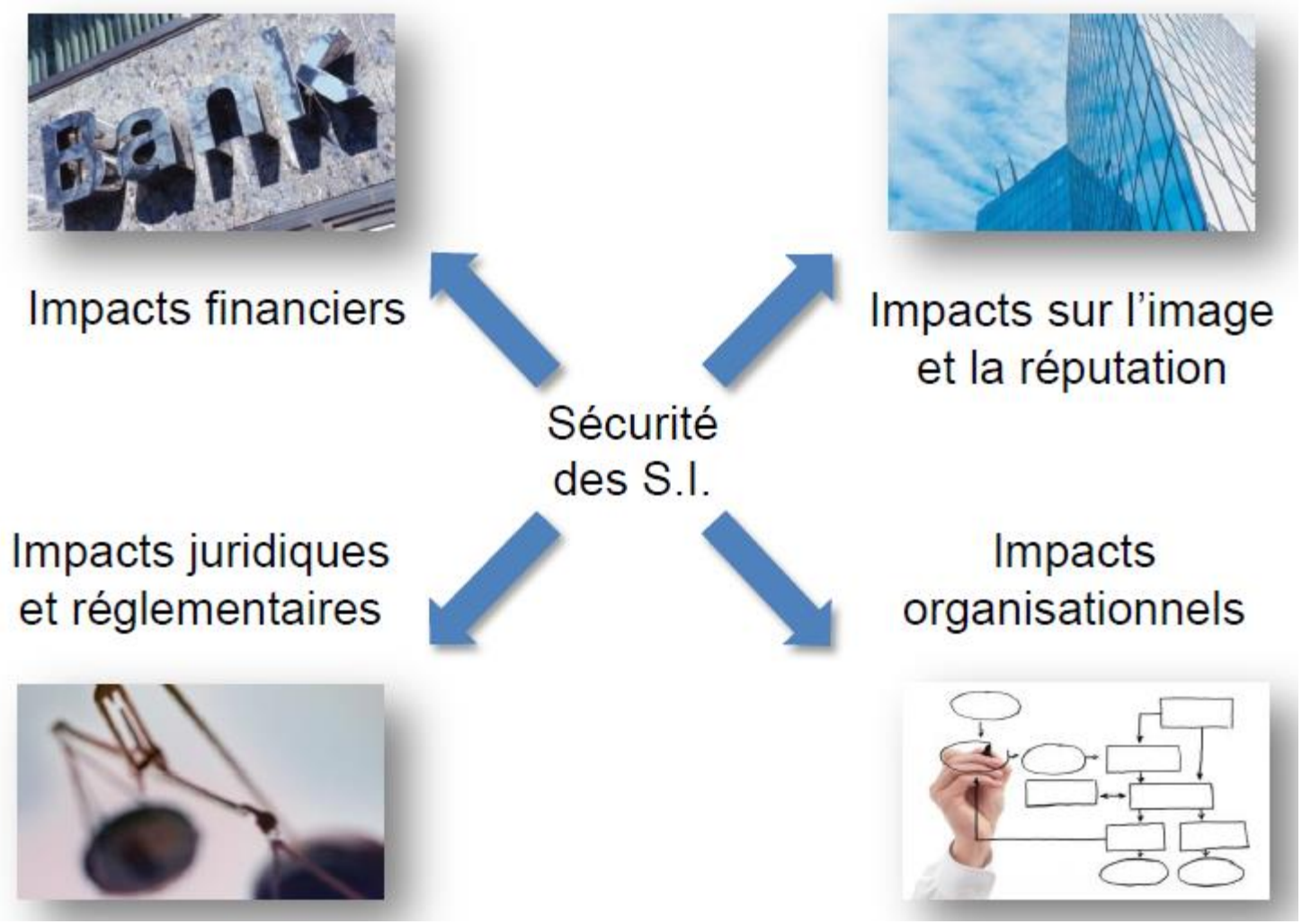


Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations,

- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
  - Elle **contribue à la qualité de service** que les utilisateurs sont en droit d'attendre
  - Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

Les enjeux (suite)



Les enjeux (suite)

- **Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus?**

- Gains financiers (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires

- Utilisation de ressources (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)

- Chantage
  - Déni de service
  - Modifications des données

- Espionnage
  - Industriel / concurrentiel
  - Étatique

Les enjeux (suite)

- **La nouvelle économie de la cybercriminalité**

Quelques chiffres pour illustrer le marché de la cybercriminalité

de 2 à 10 $	le prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays et des plafonds
5 $	le tarif moyen de location pour 1 heure d'un **botnet**, système permettant de saturer un site internet
2.399 $	le prix de commercialisation du **malware** « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $)

Introduction à la Sécurité des Systèmes d'Information
Les enjeux (suite)

- **Quelques exemples d'attaques**

Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as big an issue as traditional safety features. Photograph: Jim Dyson/Getty Images

Three months since the first fatal crash involving a Tesla driving in autopilot mode, hackers have taken remote control of a Tesla Model S from a distance of 12 miles, interfering with the car's brakes, door locks, dashboard computer screen

20 septembre 2016

Home / Lifestyle / Techno et sciences

12.10.2018, 19:55

Facebook: la faille de sécurité découverte en septembre a exposé les données de 29 millions d'utilisateurs

Réagir à cet article

SÉCURITÉ La récente faille de sécurité découverte par Facebook a finalement touché d'utilisateurs que prévu. Le réseau social estimait leur nombre à 50 millions. Ce finalement 29 millions de comptes qui ont été exposés.

Une faille de sécurité découverte en septembre dans le premier réseau social du mo a permis à des pirates informatiques de compromettre des données personnelles d quelque 29 millions d'usagers, a indiqué Facebook, bien moins qu'il ne le craignait initialement.

Facebook a précisé vendredi dans un communiqué que 15 millions de personnes ava vu leur nom et leurs contacts personnels compromis et que des détails supplément l'avaient aussi été pour 14 millions d'autres usagers. Facebook avait parlé de 50 mil de comptes compromis en révélant l'affaire le 28 septembre.

Septembre 2018

Cybersecurity

First American Financial May Have Leaked Hundreds of Millions of Re

By Noah Buhayar and Nathan Crooks

24 mai 2019 à 23:31 UTC+2 *Updated on 25 mai 2019 à 01:49 UTC+2*

- Unauthorized access to records for mortgage deals back to 2003
- First American Financial says it has fixed online weakness

First American Financial Corp. headquarters in Santa Ana, California. *Photographer: Tripplaar/Sipa via AP*

LISTEN TO ARTICLE

▶ 2:25

First American Financial Corp., one of the largest U.S. title insurers, may have allowed unauthorized access to more than 885 million records related to mortgage deals going back to 2003, according to a security researcher.

Mai 2019

Eléments clé

- **Sécurité de l'information:**
  Les mesures de sécurité doivent répondre aux besoins, missions et objectifs de l'Organisation.

  – **Chaque Organisation a des caractéristiques spécifiques:**
    - Environnements Métier différents (risque inhérent et plus ou moins grande tolérance au risque)
    - Environnements Techniques différents (S.I. plus ou moins homogène)
    - Capacités internes plus ou moins importantes (budgets, compétences…).
    - Culture d'entreprise propre à chaque organisation (notion de « risk appetite »)
    - Caractéristiques des individus.

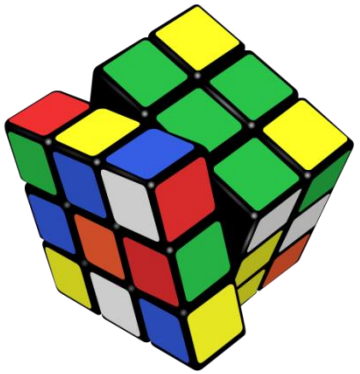
  – **Doit être gérable par les ressources disponibles** (moyens humains et techniques limités)
    (Le risque zéro n'existe pas, ne peut que tendre vers -> **loi de Murphy)**

  – **Doit être soutenable dans le temps** (**organisation par processus** pour ne pas trop dépendre des individus)

La sécurité de l'information doit donc être organisée avec des **objectifs clairs**, répondant à des **risques identifiés et évalués**, afin d'assurer une protection **suffisante** des **actifs**, qui soit **pertinente en terme de ressources** (« cost effective ») et **soutenable** dans le temps.

II) DEFINITIONS ET CONCEPTS FONDAMENTAUX

- Critères: C I D
- Types de contrôles
- le cycle de vie de l'information



Mesures techniques pour sécuriser le S.I.

C

I

D

Définitions et concepts fondamentaux

- **Les trois critères fondamentaux assurant la sécurité de l'information**

Confidentialité

Assure que seuls les utilisateurs et/ou les systèmes autorisés peuvent accéder aux données protégées.

Intégrité

Assure que les données ne peuvent être modifiées durant leur stockage ou leur transfert, et que seules des modifications autorisées peuvent être apportées aux données protégées.

Disponibilité

Assure que les systèmes et l'information sont disponibles en cas de besoin (protection contre les risques d'indisponibilité).

- Chaque facteur assure une protection différente et complémentaire de l'information.
- Ces trois facteurs doivent être maintenus de manière suffisante pour garantir que l'information et les systèmes protégés peuvent être utilisés de manière fiable.

Définitions et concepts fondamentaux

- **Quelques exemples**

Identifier les critères de sécurité impactés (C, I, D?)

	C	I	D
• Des données sensibles sont transmises à un utilisateur externe par un canal non-chiffré (ex: HTTP, e-mail).			
• La base de données de l'application e-banking ainsi que les journaux transactionnels sont sauvegardés une fois par jour sur un support externe.			
• Les correctifs de sécurité ne sont pas installés régulièrement sur les serveurs et postes de travail.			
• Les mots de passe des comptes génériques utilisés pour administrer les serveurs de Production sont conservés dans un fichier Excel partagé entre les membres du service informatique.			
• Les employés peuvent accéder aux clés USB sur leurs postes de travail mais en lecture-seule.			
• Les employés peuvent accéder sans restriction (lecture et écriture) aux clés USB sur leurs postes de travail.			
• Toutes les données du serveur de Production, dont certaines données sont sensibles (ex: numéros de carte de crédits), sont répliquées chaque jour sur le serveur de Test.			
• Les sauvegardes des données sensibles sont conservées sur des supports non-chiffrés et transportées à l'extérieur chaque semaine par une société de sécurité spécialisée.			
• Le plan de secours informatique n'a pas fait l'objet d'un test complet depuis 3 ans. Toutefois, aucun changement majeur n'a eu lieu depuis selon le responsable informatique.			

Que retenir de ces exemples?

Définitions et concepts fondamentaux

- **D'autres critères assurant la sécurité de l'information (contexte transactionnel / e-Business)**

PREUVE

Authenticité

Assure que les données, transactions, communications et documents sont bien authentiques, et que chacun des intervenants est bien celui qu'il dit être.

• Utilise la technologie du certificat numérique.

Non-répudiation

Prouve pour une transaction que les données ont été envoyées par l'expéditeur légitime (*non-répudiation de l'origine*) et reçues par leur destinataire légitime (*non-répudiation de l'arrivée*).

• Utilise la technologie du certificat numérique.

• **(option)** Possibilité de donner une valeur juridique à l'écrit électronique et à la signature électronique sous certaines conditions précises.

Contrôles

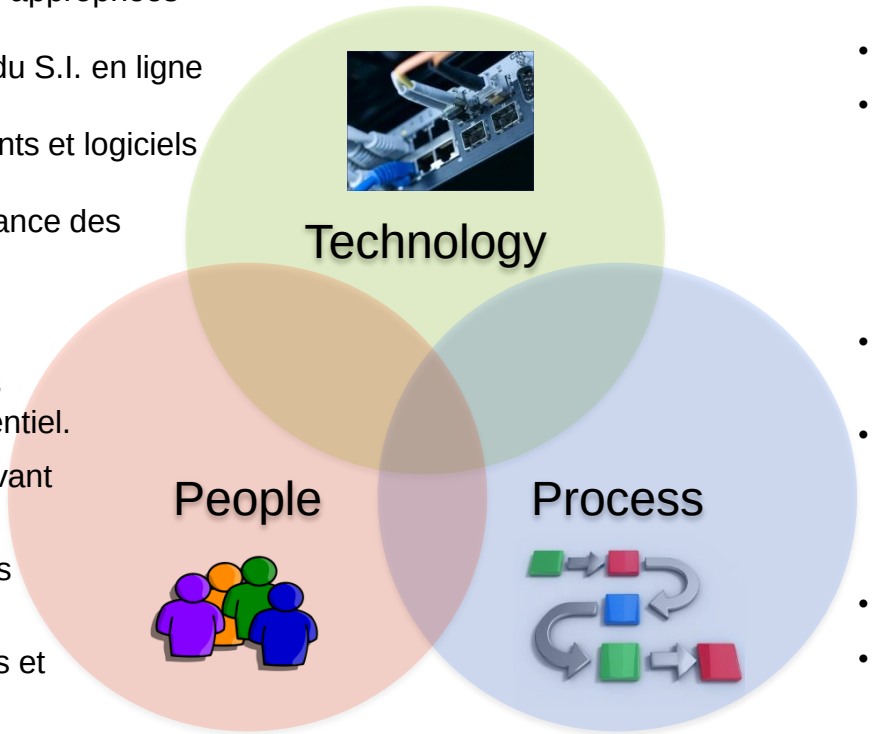
Définitions et concepts fondamentaux

- **L'environnement de contrôle interne**

  Ensemble des éléments humains, organisationnels et techniques mis en place pour **réduire les risques.**

People | **Process** | **Technology**

- Utilisation de technologies appropriées et maîtrisées.
- Capacité et performance du S.I. en ligne avec besoins Métier.
- Mise à jour des équipements et logiciels lorsque nécessaire.
- Enregistrement et surveillance des évènements de sécurité.



- Recrutement de collaborateurs expérimentés ou ayant du potentiel.
- Vérification des antécédents avant embauche si besoin.
- Formation et sensibilisation des employés.
- Communication claire des rôles et responsabilités.
- Support de la Direction Générale.

- Organisation formalisée
- Procédures et Standards pour la sécurité du S.I. assurant un fonctionnement homogène dans le temps. ***(réduire la dépendance envers quelques individus)***
- Classification des données de l'entreprise.
- Gestion standardisée des accès, des incidents, des configurations et des changements.
- Analyse des risques.
- Organisation alignée sur référentiels (p. ex. ISO27001)
- Suivi de l'exécution et Audits de la sécurité du S.I.

People – exemple de mauvais comportement

(Vu dans le train en Suisse le 3 octobre 2018)

Facteurs de risque supplémentaire:
- Compartiment de train (idéal pour cibler un vol de données)
- 1ère classe (données Business)
- Pas d'écran de veille
- Token d'authentification forte connecté

Définitions et concepts fondamentaux

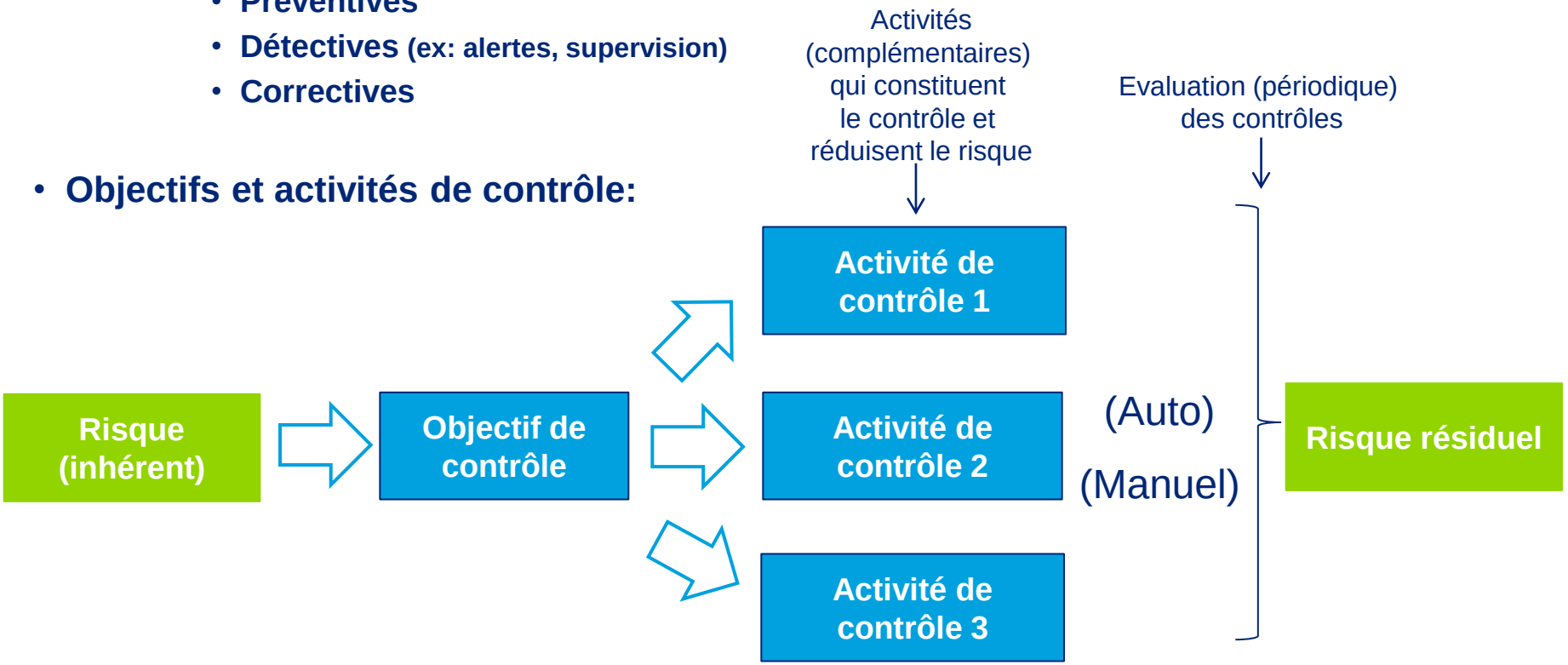
- **L'environnement de contrôle interne**

People		Process		Technology		Résultat prévisible
✓	+	✓	+	✓	=	**Succès du contrôle**
✗	+	✓	+	✓	=	Adoption faible du contrôle (ou contournement)
✓	+	✗	+	✓	=	Fonctionnement opérationnel inconsistant
✓	+	✓	+	✗	=	Difficulté à exécuter le contrôle à grande échelle
✗	+	✗	+	✓	=	Outil de contrôle acquis mais non-intégré
✗	+	✓	+	✗	=	Efforts inutiles
✓	+	✗	+	✗	=	Incapacité à exécuter
✗	+	✗	+	✗	=	Absence de défenses

Définitions et concepts fondamentaux

- **Objectif du contrôle interne IT:**
  - Réduire les risques pour obtenir une assurance ***raisonnable*** que les **objectifs Métier** de l'Entreprise seront atteints.
  - Réduire les risques par des mesures:
    - **Préventives**
    - **Détectives (ex: alertes, supervision)**
    - **Correctives**

- **Objectifs et activités de contrôle:**



Définitions et concepts fondamentaux

- **Quelques exemples de contrôles**

ISACA

	Dissuasif	Préventif	Détectif	Correctif	Compensatif	Recouvre-ment
Adminis-tratif	Politique de sécurité	Procédure de gestion des utilisateurs	Revue des rapports d'exception	Licenciement / avertissement	Supervision, rotations de personnel	Plan de secours informatique
Technique	Message d'avertissement	Mots de passe, IPS, surf control	Logs, IDS	Fermeture de session, isolation	Logs, videosurveil-lance, traçabilité	Sauvegardes des données
Physique	Panneau « Attention au chien »	Clôture d'enceinte, vitres fumées	Videosurveil-lance, détecteurs de mouvement	Extincteur	Défense échelonnée	Reconstruction

Londres 17 octobre 2012 07:02; *Act: 17.10.2012 10:30*

Le système de contrôle d'UBS était défectueux

Le système de contrôle interne d'UBS était déficient au moment où son ex-courtier Kweku Adoboli perdait plusieurs milliards, a expliqué mardi le chef du contrôle des risques de la banque suisse devant la justice londonienne.

1|14 01.05 L'autorité de tutelle financière britannique a annoncé jeudi avoir interdit d'exercice un ancien trader d'UBS pour n'avoir pas encadré correctement son collègue moins expérimenté, Kweku Adoboli.

Photo: AFP/Justin Tallis

on off *i*

En principe, le système était fiable, mais il n'a pas fonctionné comme il le devait dans certaines sections, a ajouté M. Bell, en partie à cause d'une erreur humaine.

Selon Colin Bell, Kweku Adoboli a eu au moins une fois la possibilité de signer lui-même les ordres lorsque le système de la banque les vérifiait.

Colin Bell faisait partie de l'équipe de quatre membres qui a contrôlé le processus après que l'entreprise a pris connaissance des pertes.

2 milliards de dollars

Le courtier d'origine ghanéenne âgé de 32 ans est accusé d'une fraude ayant coûté à UBS 2 milliards de dollars (environ 1,85 milliard de francs). Il est poursuivi pour «abus de position» et «fraudes comptables».

Sur ce sujet

Procès UBS : Un collègue de l'ex-trader a pensé au suicide

Procès UBS: Un témoin décrit la panique au sein d'UBS

UBS: L'ex-trader aurait embrouillé le comptable

UBS: L'ex-trader a semé le «chaos»

Les 10 nuits en enfer de Maersk pour réinstaller 4000 serveurs et 45000 PC

Sécurité : *Le transporteur a été frappé de plein fouet en 2017 par le ransomware NotPetya (Petya), avec pour conséquence la perte de 300 millions de dollars de chiffre d'affaires. Lors du World Economic Forum, Maersk a précisé avoir dû réinstaller toute son infrastructure, 4.000 serveurs, 45.000 PC et 2500 applications.*

Par Christophe Auffray | Lundi 29 Janvier 2018

Le ransomware se propageait en effet dans ses systèmes IT cœur de métier.

Le transporteur a été contraint dans ce cadre de stopper ses opérations. Et pour redémarrer, comme l'a expliqué son président Jim Hagemann Snabe lors du Forum économique mondial, l'entreprise a dû réinstaller l'ensemble de son infrastructure.

Dans un "effort héroïque", d'après les mots du dirigeant, les équipes IT ont donc réinstallé 4.000 serveurs, 45.000 PC et 2.500 applications.

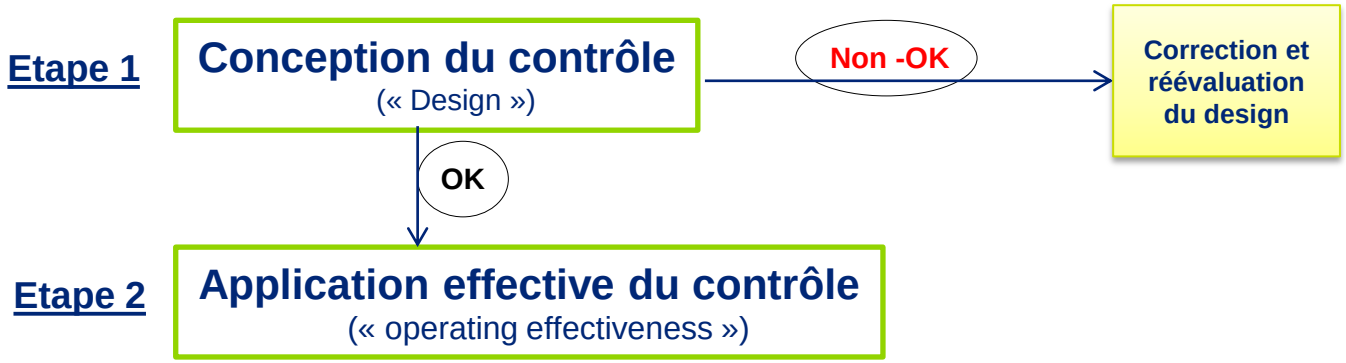
"Imaginez une entreprise où un navire de 10 à 20.000 conteneurs entre dans un port toutes les 15 minutes, et pendant 10 jours, vous n'avez pas d'informatique" a commenté Hagemann. "C'est presque impossible à imaginer. »

source: www.zdnet.fr

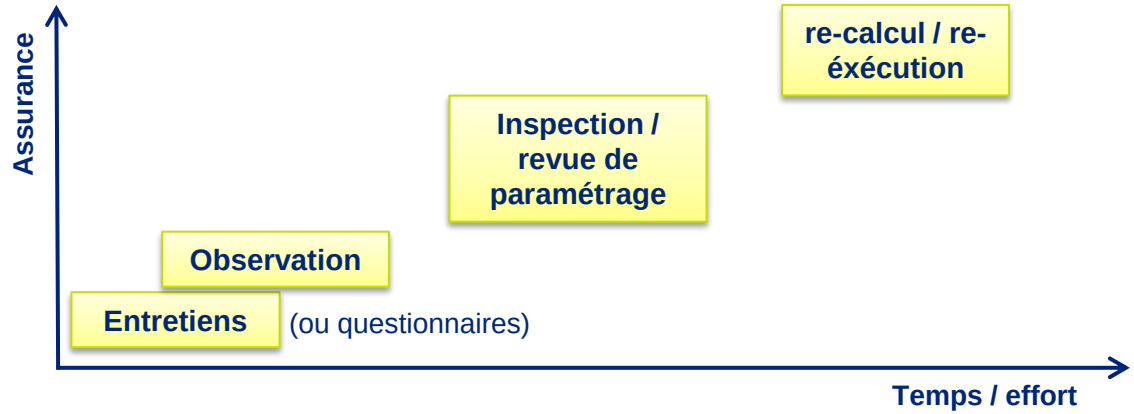
Définitions et concepts fondamentaux

- **Méthodes d'évaluation des contrôles:**
  - **1er niveau: contrôle continu par équipes opérationnelles** (ex: contrôle intégré au processus)
  - **2nd niveau: contrôle périodique indépendant** (ex: audit)

- **L'évaluation des contrôles**



- **Types d'évaluations et assurance:**



- **Exemple de critères pour évaluer et documenter la conception d'un contrôle:**

Risque R2 - Contrôle C1A - conception du contrôle: ***Objectif du contrôle***	
Décrire le travail réalisé: • Entretien avec **X** et **Y** (préciser noms et fonctions) le <date> pour revoir le fonctionnement du contrôle **Z**. • Présenter le contrôle (quelques phrases pour décrire son contexte et son objectif) • Mentionner les procédures et politiques de sécurité applicables. • Décrire le contrôle de manière explicite (QUI / QUOI / QUAND / COMMENT). **Répondre aux 5 questions ci-dessous de manière synthétique.** • Joindre des exemples de chaque contrôle observé pour référence (par ex. copies d'écran annotées) et de chaque exception relevée.	
a) est-ce le contrôle **approprié** pour réduire le risque en question?	OUI / NON - Le contrôle Z permet de réduire / ne permet de pas de réduire suffisamment le risque R2. *Guide de l'auditeur: le contrôle, s'il appliqué correctement, réduirait-il le risque inhérent en question et est-il pertinent vis-à-vis de l'objectif de contrôle? Est-ce que les objectifs de ce contrôle sont alignés avec la tolérance d'erreur pour ce contrôle (s'il y en a une)?* *Est-ce que certains contrôles manquent (par ex. est-il nécessaire d'avoir un contrôle préventif **et** un contrôle détectif?)*
b) est-ce que le contrôle est conçu pour être **réalisé à la bonne étape** du processus? Est-ce que sa fréquence est la bonne?	OUI / NON - expliquer *Guide de l'auditeur: Le contrôle devrait-il être préventif, détectif, ou une simple supervision?* *Pour des processus à risque élevé, un contrôle détectif est-il suffisant?* *La fréquence (ex. mensuelle, quotidienne) est-elle suffisante?*
c) Le contrôle est-il **soutenable** dans le temps?	OUI / NON - expliquer *Guide de l'auditeur:* ➢ *Si le contrôle est automatisé: OUI, car le contrôle n'est pas impacté par dex augmentations de volumes, ou par une dépendance envers des personnes clés.* ➢ *Si le contrôle est manuel, fonctionnerait-il toujours correctement en cas d'augmentation des volumes? Y a-t-il des périodes de charge pouvant créer des exceptions? Y a-t-il des procédures, des remplaçants, des formations pour ne pas dépendre excessivement d'une personne clé?*

Définitions et concepts fondamentaux

• Exemple de critères pour évaluer et documenter la conception d'un contrôle:

d) le contrôle est-il réalisé par les **bonnes personnes** et par le bon niveau dans l'organisation?	OUI / NON - expliquer *Guide de l'auditeur:* ➢ *Si le contrôle est automatisé: **Non-Applicable** car contrôle automatisé,.* ➢ *Si le contrôle est manuel, la personne réalisant le contrôle est-elle appropriée? Y a-t-il un conflit d'intérêt? Y a-t-il une nécessité de faire intervenir deux personnes différentes (ségrégation des tâches)? La seconde personne a-t-elle suffisamment d'expérience pour juger (si principe de « maker / checker »)?*
e) Le contrôle est-il associé à des **preuves**, est-il matérialisé?	OUI / NON - expliquer *Guide de l'auditeur: Si le contrôle est automatisé: y a-t-il un journal d'événements (« audit trail ») dans l'application?* *Si le contrôle répond à une exigence réglementaire, y a-t-il suffisamment de documentation prouvant que le contrôle est réalisé (ex. e-mail, signature par la personne qui revoit). Si non, existe t-il d'autres informations permettant de prouver que le contrôle est bien réalisé?*

Si une des réponses aux 5 questions est « NON », alors la conception du contrôle n'est pas considérée comme appropriée et une exception doit être remontée.

• Exemple de tests réalisés pour vérifier que le contrôle est appliqué:

Contrôle manuel: évaluation par d'échantillonnage
(exemple: contrôle hebdomadaire -> revue de 12 occurrences du contrôle
(*Taille à définir selon la fréquence du contrôle)

Contrôle automatique:
- ❑ **Option 1: test d'une occurrence,** par ex. vérification qu'une personne ne peut pas autoriser ses propres saisies
- ❑ **Option 2: revue de paramétrage** (droits d'accès, niveaux d'autorisations, etc.)
- ❑ **Option 3: recalcul / analyse de données / revue des journaux d'évènements**

(*Option à définir au cas par cas selon le niveau d'assurance requis)

Conclusion finale:
En pratique, le contrôle est-il effectivement réalisé comme il se doit, par les bonnes personnes, systématiquement et sans anomalies ?

- ➢ **OUI**: le contrôle est considéré effectif (pas d'exceptions).
- ➢ **NON / Partiellement:** quantifier les déviations, analyser les causes, rapporter les anomalies, traiter les risques et les causes.

Le cycle de vie de l'information

Le cycle de vie de l'information

- **Objectif:**
  - Gestion rationnelle du patrimoine d'information de l'entreprise en fonction de la valeur de l'information et du coût de son stockage:
    - Rationnaliser les moyens de stockage de l'information suivant les exigences techniques, réglementaires et juridiques les plus adaptées pour stocker et rendre disponible l'information
    - Assurer un suivi du cycle de vie des documents

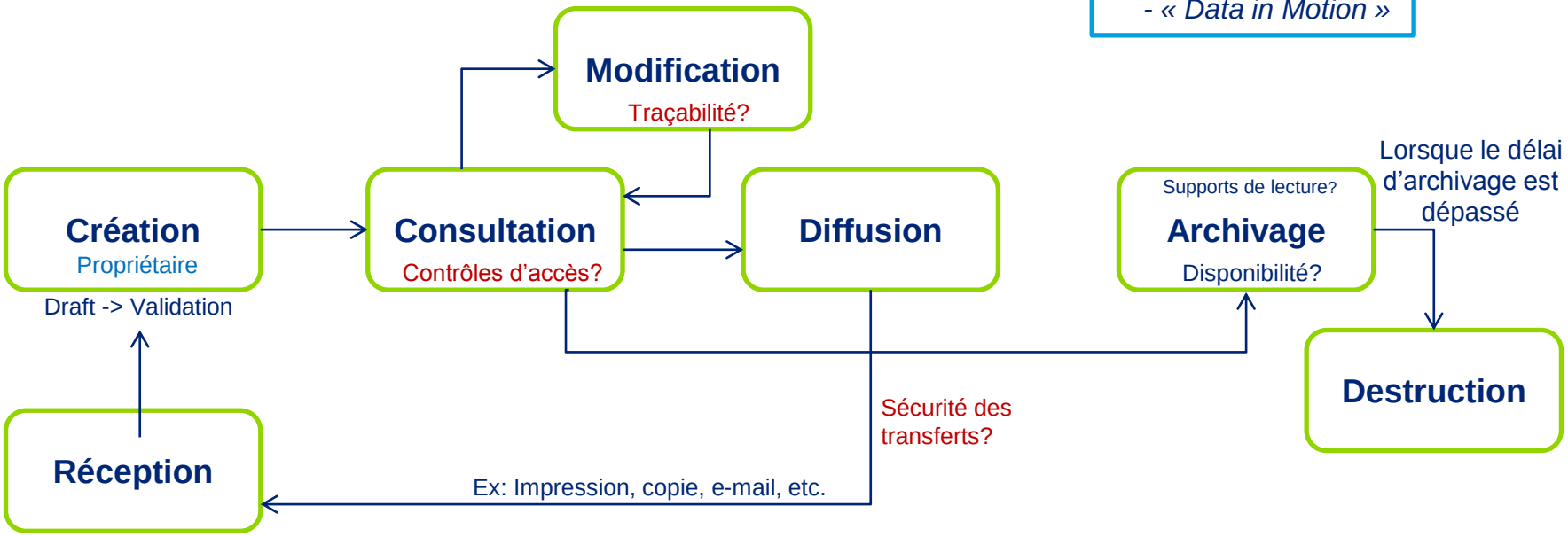
  - **Etapes du cycle de vie des documents:**
    - Création du document
    - Modification du document
    - Transfert de l'information (copie)
    - Conservation
    - Consultation
    - Accès distant
    - Archivage
    - Destruction (End of Life)

Challenge: **Trouver le meilleur compromis entre disponibilité et valeur de l'information**

Le cycle de vie de l'information

Gartner:
- *« Data at Rest »*
- *« Data in Use »*
- *« Data in Motion »*

- **Le cycle de vie des documents:**



- **Challenges:**

Aspects sécurité — Niveau de classification qui évolue au cours du cycle de vie d'un document (-> évolution des besoins sécurité).

Aspects légaux — Protection: données personnelles, données de cartes de crédit, etc. Rétention: transactions, documents comptables, etc.

→ Lois? Règlements? Contrats?

Compromis coût / disponibilité — (Ex: archivage des transactions pendant 2 ans sur support haute-disponibilité, puis 5 ans sur support « low cost » avant destruction.

Questions?