Audit de la Sécurité des S.I.

Introduction

1

Préambule

1. Introduction : objectifs, référentiels, risques
2. Les démarches de contrôle
3. Les investigations
4. La restitution
5. La professionnalisation du métier d'auditeur

2

1 - Introduction

⇨Définitions

⇨Qualités et éthique

⇨Objectif des contrôles

⇨La notion de référentiel
- ✓Environnement juridique
- ✓Les normes et bonnes pratiques

⇨Points clés

3

Quizz

1 – A quand remonte les premiers audits

- ❑ Au temps de romains.
- ❑ Sous Louis IV.
- ❑ Suite au Crach boursier de 1929

4

Audit & contrôle

Définitions

Un peu d'histoire …

- **Période Romaine**
  - •Audit, du latin « audire » : écouter. Utiliser pour le contrôle au nom de l'empereur sur la gestion des provinces
  - •Synonyme : contrôle, vérification, expertise, évaluation, etc.

- **XIIIe siècle** :
  - • Notion anglo-saxonne visant la gestion. Premier cabinet d'audit à Londre
  - • Chambre des comptes en France en 1319

5

Audit & contrôle

Définitions

Saint Wikipedia (2013)

L'**audit** est l'examen **professionnel** qui consiste en une **expertise** par un agent **compétent** et **impartial** aboutissant à un jugement sur les états financiers, le contrôle interne, l'organisation, la procédure, ou une opération quelconque d'une entité.

6

Audit & contrôle

Définitions

IFACI (Institut Français de l'Audit et du contrôle Interne)

⇨ L'Audit *Interne* est une activité **indépendante** et **objective** qui donne à une organisation une **assurance sur le degré de maîtrise** de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.

➢ L'audit aide cette organisation à atteindre ses objectifs en évaluant, par une approche **systématique** et **méthodique**, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité.

7

Audit & contrôle

Définitions

International Organization for Standardization

⇨ L'audit est un processus systématique, **indépendant** et **documenté** en vue d'obtenir des **preuves d'audit** (enregistrements, énoncés de faits ou autres informations, qui se rapportent aux critères d'audit et sont **vérifiables**) et de les évaluer de manière **objective** pour déterminer dans quelle mesure les critères d'audit (ensemble de politiques, procédures ou exigences déterminées) sont satisfaits

⇨ Audit Première partie, Audit Seconde partie, Audit Tierce partie :

⇨ **norme ISO 19011 (version 2002).**

8

Définitions

- **Audit de conformité** : audit pour démontrer le respect de certaines normes, politiques, règlements, lois, …
- **Audit financier** : audits visant à évaluer la justesse des rapports financiers
- **Audits opérationnels** : audits visant à évaluer le contrôle interne
- **Audits des S.I.** ; audits visant à recueillir des preuves pour déterminer si le SI protège adéquatement les actifs (DICT), fournit des renseignements pertinents et fiables, atteint les objectifs métiers, …
- **Audits spécialisés** : normes particulières (SSAE 16 : externalisation par exemple)
- **Investigation légale** : audit spécialisé dans la découverte, la divulgation et le suivi des fraudes et des crimes

9

Qualités et Ethique

- **Déontologie :**
  - Le fondement du professionnalisme
  - La confiance, l'intégrité, la confidentialité et la discrétion
  - La loyauté (« pas de pièges »)
- **Impartialité et transparence**
- **Conscience professionnelle**
  - L'attitude diligente et avisée au cours de l'audit
- **Indépendance**
  - La fondement de l'impartialité de l'audit et de l'objectivité des conclusions d'audit

10

Qualités et Ethique

⇨**Compétences**

⇨Approche fondée sur la **preuve**
- ⇨La méthode rationnelle pour parvenir à des conclusions d'audit fiables et reproductibles dans une processus d'audit systématique
- ➢Basé sur des faits et non des inférences
- ➢Preuves d'audit vérifiables

⇨Objectif **d'amélioration**

⇨ **Charte d'audit :** précise la fonction d'audit (règles, conditions, normes, …)

11

Quizz

1 - Mes audits de cette année doivent traiter au mieux le volet Sécurité des SI. Quelle est la meilleure solution pour être pertinent ?

- ❑ Muter un expert SSI de la Production Informatique dans le Département Audit SSI en charge du programme.
- ❑ Former mes auditeurs à la Sécurité des S.I.
- ❑ Embaucher des experts

12

Quizz

1 - Mes audits de cette année doivent traiter au mieux le volet Sécurité des SI. Quelle est la meilleure solution pour être pertinent ?

- ❑ Muter un expert SSI de la Production Informatique dans le Département Audit SSI en charge du programme.
- ❑ Former mes auditeurs à la Sécurité des S.I.
- ✓ Embaucher des experts

13

Quizz

2 Un expert a identifié une faille lors d'un test d'intrusion et a réussi à pénétrer le S.I. à partir de l'extérieur. Lors de la présentation à la Direction générale, est-il pertinent ?

- ❑ qu'il explique les opérations qu'il a réalisées.
- ❑ qu'il détaille les failles techniques identifiées et leur niveau d'exploitabilité.
- ❑ qu'il explicite les risques qui impactent l'entreprise

14

Quizz

2 Un expert a identifié une faille lors d'un test d'intrusion et a réussi à pénétrer le S.I. à partir de l'extérieur. Lors de la présentation à la Direction générale, est-il pertinent ?

- ❑ qu'il explique les opérations qu'il a réalisées.
- ❑ qu'il détaille les failles techniques identifiées et leur niveau d'exploitabilité.
- ✓ qu'il explicite les risques qui impactent l'entreprise

15

Quizz

3 L'équipe d'experts SSI a identifié au cours d'un contrôle ce qu'elle croit être une non-conformité à une règle juridique. Comment doit-elle l'intégrer dans son rapport ?

- ❑ En détaillant ce qu'elle croit être non conforme.
- ❑ En ne disant rien, car ce n'est pas de la sécurité.
- ❑ Sous forme de remarque et en suggérant de faire appel à la Direction Juridique

16

Audit & contrôle

Quizz

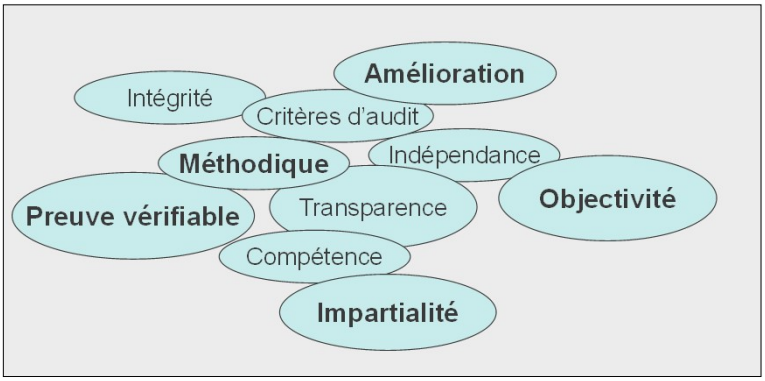
3 L'équipe d'experts SSI a identifié au cours d'un contrôle ce qu'elle croit être une non-conformité à une règle juridique. Comment doit-elle l'intégrer dans son rapport ?

- ❑ En détaillant ce qu'elle croit être non conforme.
- ❑ En ne disant rien, car ce n'est pas de la sécurité.
- ✓ Sous forme de remarque et en suggérant de faire appel à la Direction Juridique

17

Audit & contrôle

Points clefs …



18

Objectifs du contrôle SSI

⇨ Auditer : de bonnes raisons
- ✓ Obligations (CAC, administrations, règlements, …)
- ✓ Améliorer, se rassurer ...
- ✓ Évaluer / comparer
- ✓ Sensibiliser
- ✓ Analyser sur incident
- ✓ Certifier / prouver
- ✓ ..

⇨ Auditer : pour évaluer le niveau de protection ou de prise en compte d'un risque

19

Objectifs du contrôle SSI

⇨L'objectif d'un contrôle SSI va dépendre de sa nature :

✓**Conformité vis-à-vis d'une loi ou d'une norme** :
- Exemple 1 : s'assurer que la politique de sécurité est bien appliquée et vérifier que les moyens mis en œuvre sont présents.
- Exemple 2 : vérifier que la loi Informatique et Liberté est respectée
- Exemple 3 : vérifier que le sous-traitant applique les exigences de sécurité que l'entreprise a précisées dans son contrat

⇒***Mesurer, identifier un écart vis-à-vis d'un référentiel***

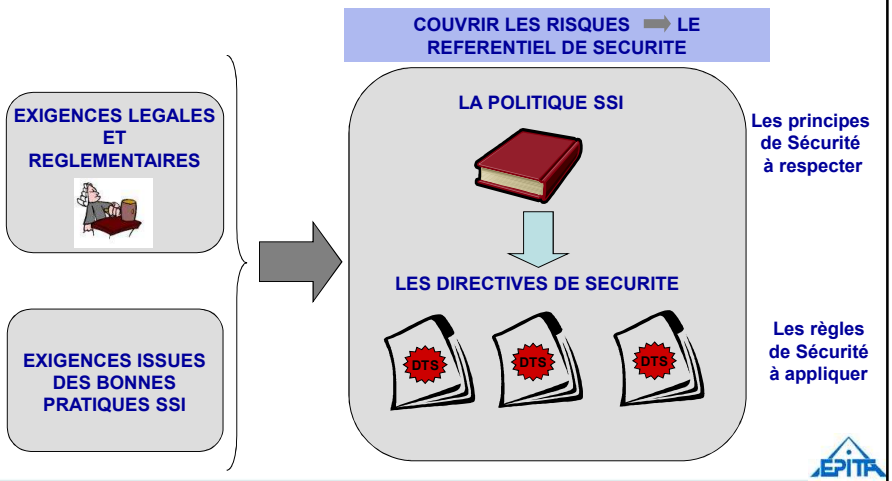
✓**De robustesse, d'efficacité, ...**
- Exemple 1 : vérifier que les moyens mis en œuvre pour protéger les données sensibles sont efficaces

⇒***Identifier un risque, une vulnérabilité, un défaut, ...***

20

Audit & contrôle

Référentiel de contrôle (critères !)



21

Audit & contrôle

Référentiel de contrôle

⇨ **Pour réaliser les contrôles, les familles de document suivantes sont à prendre en compte par ordre de priorité :**

- ✓ Les principaux textes réglementaires applicables au SI du secteur audité :
  - Cadre légal, l'ex CRBF, la CNIL, ...
  - Textes spécifiques au contexte de la cible à contrôler, par exemple : signature électronique, archivage, ….
- ✓ Les règles/ les exigences de sécurité de l'entité concernée
  - La Politique de Sécurité du SI de la Banque Postale,
  - La Directive Générale de la sécurité des SI de la DSI
  - Les Directives Techniques de Sécurité qui en sont déclinées.
  - Les procédures de sécurité qui en sont déclinés
- ✓ Les normes et règles de l'art techniques.

22

Audit & contrôle

Référentiel de contrôle

⇨ **Concernant les prestations externalisées, les principaux documents complémentaires à prendre en tant que référentiels sont** :

- ✓ Les pièces contractuelles (Plan D'assurance Sécurité, PCA, PRA, …) et Les Politiques des Sécurité rattachées
- ✓ Les règles de l'art

23

Audit & contrôle

Référentiels Réglementaires

⇨ **Loi I&L**

- ✓ Protection des données à caractère personnel (DCP). Sont considérées comme DCP toute information relative à une personne physique identifiée ou qui peut être identifiée (loi 78 Informatique & Libertés)
- ✓ Obligation de sécurisation des DCP

• Finalité et proportionnalité du traitement • Information des personnes impactées • Limitation de la durée de conservation • Communication des mesures mises en œuvre • Autorisation pour certains traitements (Biométrie, Données de santé, …)	• Cloisonnement, • Gestion des droits d'accès, • Protection des données stockées, • Gestion des durée de rétention • **Contrôle de l'efficience** • …

24

Audit & contrôle

Référentiels Réglementaires

« DCP : *Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement ».*

- **identification directe** : nom, prénom, photographie, image sur bande vidéo ;


- **identification indirecte** : numéro de téléphone, numéro de CB, numéro de compte bancaire, empreinte digitale, etc.

25

Audit & contrôle

Référentiels Réglementaires

Une Directive européenne insuffisamment efficace : trop de libertés données aux États membres

- En Allemagne, un très important formalisme
- En Espagne, des sanctions très fortes
- Au Royaume-Uni, des traitements possibles sans information préalable (contrôle clandestin des salariés) ;.

Une évolution nécessaire : Big Data, Cloud , sanctions financières peu élevées, …

26

Référentiels Réglementaires

Nouveau Règlement européen sur la protection des données personnelles

Les grands principes inchangés :
- Loyauté, finalité, proportionnalité
- Les données sensibles
- Les pouvoirs opérationnels de la CNIL
- L'analyse de risque pour les droits et libertés des personnes physiques;.

Une évolution nécessaire :
- Le renforcement des droits des personnes (effacement, portabilité, …)
- *Accountability* (Traçabilité, Preuve, audits)
- *Privacy by design / by default*
- L'analyse d'impact pour les traitements « à risque élevé »
- La notification des violations
- Co-responsabilité du sous-traitant
- Sanctions financières : 20 000 000 € ou jusqu'à **4 % du CA**…

27

Référentiels Réglementaires

⇨**Code du travail**
- ✓ Proportionnalité des mesures
- ✓ Transparence dans la mis en place des mesures
- ✓ Discussion collective
  - •Information des salariés
  - •Information / Négociation des partenaires sociaux (C.E.)

⇨ **Directive NIS, Loi de Programmation Militaire**
- ✓ Audit et contrôle pour homologation

⇨ **SOX, COSO (en réponse aux scandales Exon, …)…**

⇨ **Les contrats**

28

Référentiels Normatifs

⇨ **Les Normes, Bonnes pratiques, Recommandations, …**

- ⇨ ISO 27xxx (normes SSI)
- ⇨Recommandations de l'ANSSI
- ⇨COBIT (Pilotage S.I.)
- ⇨ ITIL (Organisation Production)
- ⇨ SAS 70 (extern.)
- ⇨ OWASP

29

Obligations de contrôle

⇨ **Directive NIS, Loi de Programmation Militaire**
- ✓ Audit et contrôle pour homologation

⇨ **SOX en réponse aux scandales Exon, …)…**
- ✓ Contrôle des droits et des habilitations

⇨ **Les contrats**
- ✓ Clauses d'audit

30

Obligations de contrôle

Réglementation bancaire :

- ⇨ La réglementation bancaire (ex CRBF 97-02) impose l'existence d'un dispositif de contrôle interne. Le contrôle SSI s'intègre dans ce dispositif.
- ⇨ Le dispositif de contrôle interne comporte :
  - ✓ Le contrôle permanent, mené à tous les niveaux
    - opérationnels,
    - management,
    - unités spécialisés non opérationnelles.
  - ✓ Le contrôle périodique
    - C'est l'Inspection Générale.
    - C'est le contrôle des contrôles.

31

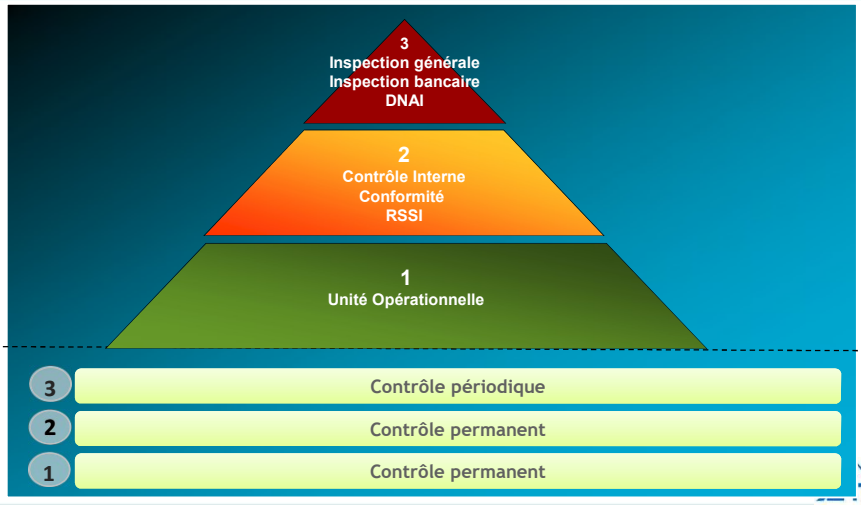
Obligations de contrôle

- ⇨ **Il y a généralement deux niveaux de contrôle permanent :**
  - ✓ niveau 1 : contrôles menés par les opérateurs
  - ✓ niveau 2 : contrôles menés
    - Par le management
    - Par des contrôleurs intégrés aux métiers
    - Par des entités non opérationnelles. Le RSSI et son équipe (si elle n'a pas de rôle opérationnel) constituent une unité de contrôle N2.
- ⇨ **Le RSSI est un acteur du contrôle permanent. Ses contrôles**
  - ✓ vérifient que les contrôles de niveaux inférieurs
    - existent,
    - reflètent la réalité.
  - ✓ apportent des certitudes qui ne soient pas simplement issues de la consolidation des contrôles de niveau inférieur

32

Audit & contrôle

Obligations de contrôle



33

Audit & contrôle

Obligations de contrôle

⇨ **Respecter le cycle PDCA, …**

34

Contrôle et Risques SSI

⇨ L'analyse du risque doit aider l'auditeur à repérer les risques afin de lui permettre d'orienter ses travaux. C'est un point d'entrée indispensable
- ✓ Pour définir un audit
- ✓ Pour prioriser un audit
- ✓ pour planifier un audit

⇨ Les résultats d'un audit peuvent alimenter les analyses de risques
- ✓ En diminuant le risque
- ✓ En augmentant le risque

35

Quizz

La Banque Locale de Martinique souhaite identifier les risques qui pèsent sur son Datacenter afin de mener un audit de contrôle. Identifier les menaces les plus probables :

- ❑ Inondation.
- ❑ Tremblement de terre.
- ❑ Feu.
- ❑ Alimentation électrique
- ❑ Intrusion
- ❑ Climatisation

36

Quizz

La Banque Locale de Martinique souhaite identifier les risques qui pèsent sur son Datacenter afin de mener un audit de contrôle. Identifier les menaces les plus probables :

- ✓ Inondation.
- ❑ Tremblement de terre.
- ❑ Feu.
- ✓ Alimentation électrique
- ❑ Intrusion
- ✓ Climatisation

Que vont vérifier les audits :

37

Quizz

Que vont vérifier les audits :

-Présence de détecteur d'humidité

-Etat de l'évacuation des eau de pluie

-Etanchéité des toits

- Conformité électrique

- Alimentation de secours, tests réalisés

- Dimensionnement de la climatisation

-Respect des cycles de maintenance

38

Audit & contrôle

Quizz

Quel est le risque majeur pour une banque:

- ❑ Fraude interne et/ou externe
- ❑ Non respect de la réglementation
- ❑ Atteinte à l'image

39

Audit & contrôle

Quizz

Quel est le risque majeur pour une banque:

- ✓ **Fraude interne et/ou externe**
- ✓ **Non respect de la réglementation**
- ❑ Atteinte à l'image

Que vont vérifier les audits :

40

Quizz

Que vont vérifier les audits :

-Présence de procédures

-Cycle de contrôle

-Moyens de surveillance

- Exigences réglementaires

41

Quizz

Quel est le risque majeur pour un hôpital :

- ❑ Disponibilité des données de santé
- ❑ Atteinte à la confidentialité et l'intégrité des informations de santé de ses patients.
- ❑ Atteinte à son dispositif de facturation

42

Audit & contrôle

Quizz

Quel est le risque majeur pour un hôpital :

- ✓ **Disponibilité des données de santé**
- ❑ Atteinte à la confidentialité et l'intégrité des informations de santé de ses patients.
- ❑ Atteinte à son dispositif de facturation

Que vont vérifier les audits :

43

Audit & contrôle

Quizz

Que vont vérifier les audits :

-Sauvegardes

-Redondances des matériels critiques

-Procédures de restauration

- Secours électrique

44

Illustration

Audit & contrôle

Cybercriminalité

Service de marketing externalisé : Orange

Impact

- ⇨ Les données personnelles de 1,3 millions de clients dérobées
- ⇨ La CNIL met en avant un défaut d'encadrement des sous-traitants…

Mode opératoire

- ⇨ Une simple modification d'adresse Internet (URL) a permis l'accès aux données

Objectif d'un audit qui aurait dû avoir lieu ?

45

Illustration

Audit & contrôle

Cybercriminalité

- ⇨ Vérifier les modalités de sous-traitance,
- ⇨ la formalisation d'exigences de sécurité
- ⇨ Vérification de la bonne application de ces dernière par la sous-traitant

46

Illustration

Audit & contrôle

Cybercriminalité

Cryptolocker dans l'hôpital (US)

Impact

- ⇨ Retour aux échanges par fax !!!
- ⇨ Hôpital paralysé pendant 10 jours qui avait dû envoyer ses patients vers d'autres centres de soin,

Mode opératoire

- ⇨ Pièce jointe dans un mail professionnel contrefait
- ⇨ Chiffrement des annuaires permettant l'échange des dossiers médicaux

Objectif d'un audit qui aurait dû avoir lieu ?

47

Illustration

Audit & contrôle

Cybercriminalité

- ⇨ Vérifier la robustesse de la messagerie
- ⇨ Vérifier l'efficacité du plan de reprise d'activité
- ⇨ Vérification des sauvegardes
- ⇨ Niveau de sensibilisation

48

Illustration

Audit & contrôle

Cybercriminalité

Vulnérabilité Site WEB : TF1

Impact

- ⇨ Vol de 1,9 millions de données clients
- ⇨ TF1 doit se mobiliser pour expliquer l'attaque à travers une forte mobilisation en matière de communication

Mode opératoire

- ⇨ Janvier 2015 : Des pirates trouvent 2 failles SQL sur le site TF1.fr, notamment sur une partie gérée par leur partenaire ViaPresse.

Objectif d'un audit qui aurait dû avoir lieu ?

49

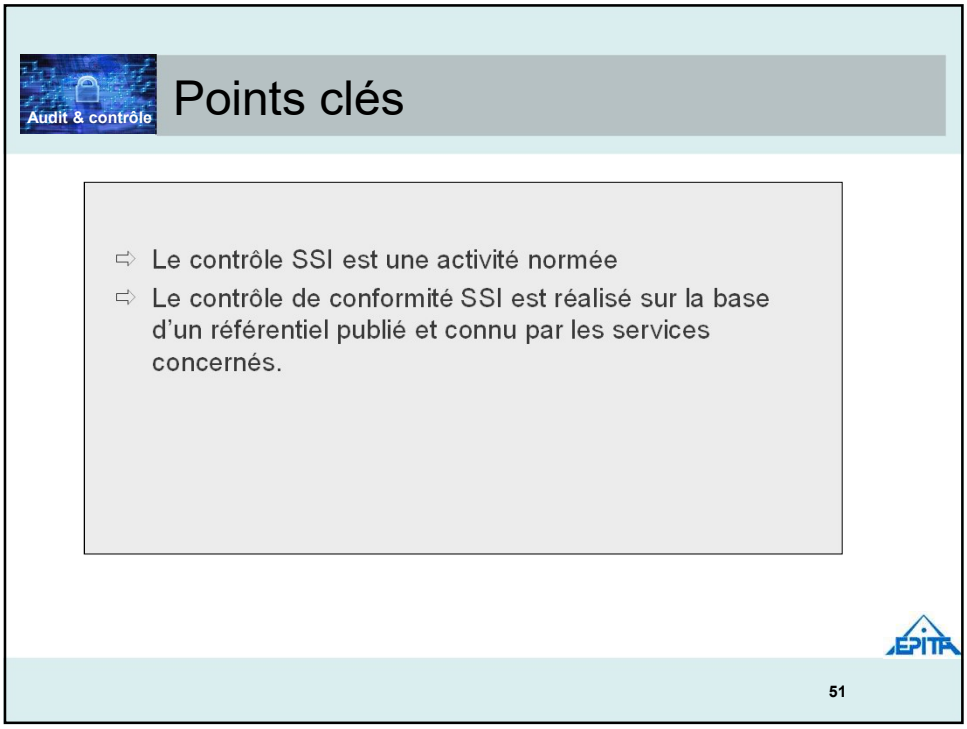
Illustration

Audit & contrôle

Cybercriminalité

- ⇨ Revue de vulnérabilité des applications WEB
- ⇨ Protection des données (chiffrement)
- ⇨ Exigences demandées au sous-traitant

50


Audit & contrôle
Points clés
Le contrôle SSI est une activité normée
Le contrôle de conformité SSI est réalisé sur la base d'un référentiel publié et connu par les services concernés.
EPITA
51