
phosforea
my learning experience

Evaluation de la sécurité

-Session Présentielle-

phosforea
my learning experience

Objectifs de la session

Comprendre quelles sont les techniques permettant l'évaluation de la sécurité et leur applications

phosforea
my learning experience

Etude de cas

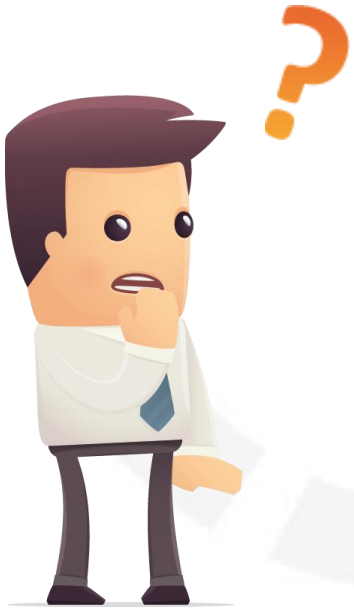
- Vous venez d'intégrer une nouvelle structure qui a subie récemment un incident de sécurité.
- Votre hiérarchie vous demande de proposer des mesures permettant d'évitant que ce type d'incident se reproduise.
- Vous devez donc réaliser un audit de sécurité de votre système et présenter votre rapport et vos recommandations à votre direction.
- Comment allez-vous procéder ?

phosforea
my learning experience

Comment procéder ?

Je cherche un plan existant pour repérer mon matériel ?

J'analyse mon système en me connectant sur chaque machine ?



J'appelle un ami...

phosforea
my learning experience

Audit sécurité

phosforea
my learning experience

Qu'est-ce qu'un audit ?

- ISO 19011, clause 3.1 :
  - Processus systématique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits
  - Exercice d'évaluation basé sur les faits

- Auditer = demander à l'audité ce qu'il fait + vérifier s'il le fait

- Note : un audit peut être organisationnel, technique ou mixte.

Objectifs de l'audit

- Mettre en relief les forces et les faiblesses de l'organisme ou du système audité (les vulnérabilités)

- Savoir si l'organisme ou le système audité est conforme à un référentiel

Acteurs de l'audit

Client	• Organisme ou personne demandant l'audit
Audité	• Organisme qui est audité
Auditeur	• Personne compétente qui réalise l'audit
Expert	• Personne qui fournit des connaissances spécifiques • Expert technique qui assiste l'équipe d'audit
Équipe d'audit	• Ensemble des personnes réalisant l'audit soutenues au besoin par les experts techniques

Guide et observateurs

Note : Les guides et observateurs ne doivent pas s'ingérer dans les discussions ou influencer l'audit

Responsabilités des guides

- Coordonner et faciliter les activités d'audit
- S'occuper des aspects logistiques
- S'assurer du respect des règles de santé et sécurité au travail
- Être témoin de l'audit pour le compte de l'audité

Présence d'observateurs

- La présence des observateurs dans l'équipe d'audit doit être approuvée par l'audité
- Ceux-ci peuvent être des auditeurs en formation ou un membre de l'organisme de certification effectuant un contrôle de qualité de l'audit

Les différents types d'audits

- Audit interne = audit première partie
  - Notre organisme audite ses propres systèmes
  - Intégré dans le processus d'amélioration continue

- Audit externe
  - Audit seconde partie
    - Deux cas de figure :
      - Notre client audite notre organisme
      - Notre organisme audite notre fournisseur
  - Audit tierce partie
    - Notre organisme est audité par un organisme indépendant
      - Ex : organismes de certification d'entreprise

Les différents enjeux des audits

- Audit d'opinion
  - Audit qui cumule évaluation de l'état ou de la conformité d'un système et des recommandations
  - Généralement effectué par les sociétés de conseil
  - Enjeu : recevoir des conseils et des recommandation pour améliorer ou rendre conforme le système audité.

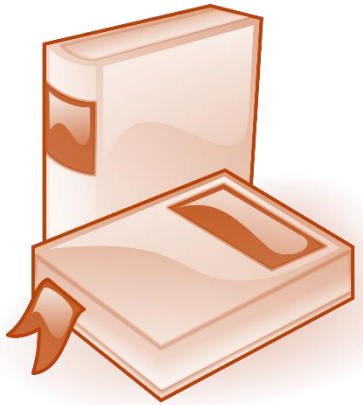
- Audit de pré-évaluation
  - audit d'évaluation de l'état ou de la conformité d'un système, sans aboutir à sa certification.
  - « audit à blanc »
  - Enjeu : préparer la certification du système

- Audit de certification
  - Audit d'évaluation de la conformité d'un système au regard d'un critère d'audit. Certification si le système répond aux critères d'audit.
  - Réalisé par un audit de certification accrédité.
  - Enjeu : recommander ou ne pas recommander la certification

Les critères d'audit

- Qu'est ce que c'est ?
  - Ensemble de politiques, procédures ou exigences utilisées comme référence vis-à-vis de laquelle les preuves d'audit sont comparées

- Les sources des critères d'audit
  - Lois, directives, règlements gouvernementaux
    - Ex : RGS, loi informatique et libertés…
  - Normes nationales
    - Ex : le NIST 800-53 pour les USA
  - Normes internationales
    - Ex : ISO27001, ISO9001, principes de l'OCDE
  - Référentiels industriels
    - Ex : PCI-DSS, HDS…
  - Politique de l'organisme



Pourquoi et quand réaliser un audit ?

- Pour évaluer son niveau de maturité en sécurité sur un périmètre défini : Évaluation de la pertinence ou du besoin de mesures de sécurité
  - Évaluation périodique dans le cadre de l'amélioration continue
    - Recommandation : 1f/an
  - Évaluation ponctuelle
    - Suite à incident de sécurité
    - Suite à changement impactant dans le SI (recours au Cloud, à la virtualisation…)
- Pour évaluer la conformité avec une norme, politique, réglementation
- Pour préparer une certification

phosforea
my learning experience

Les audits techniques de sécurité

- Il en existe 5 types :
  1. Test d'intrusion
  2. Audit d'architecture
  3. Audit de configuration
  4. Audit de code source
  5. Audit organisationnel et physique

Les tests d'intrusion

- **Principe** : découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel.

- **Remarque** : un test d'intrusion seul n'a pas vocation à être exhaustif. Il peut, en effet, être réalisé en complément d'autres audits (en général, audit de code) afin d'en améliorer l'efficacité ou de vérifier l'exploitabilité d'une vulnérabilité.

Audit d'architecture

- **Principe** : vérifier la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information par rapport à l'état de l'art et aux exigences et règles internes de l'audité.

- L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

Audit de configuration

- **Principe** : vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information.

Audit de code source

- **Principe** : analyser tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

Audit organisationnel et physique

- **Principe** :
  - S'assurer que les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information sont conformes aux besoins de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur.
  - S'assurer qu'elles complètent correctement les mesures techniques mises en place.
  - S'assurer qu'elles sont efficacement mises en pratique.
  - S'assurer que les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

Principes d'audit

- ISO 19011, Clause 4

Déontologie 4A

Présentation impartiale 4B

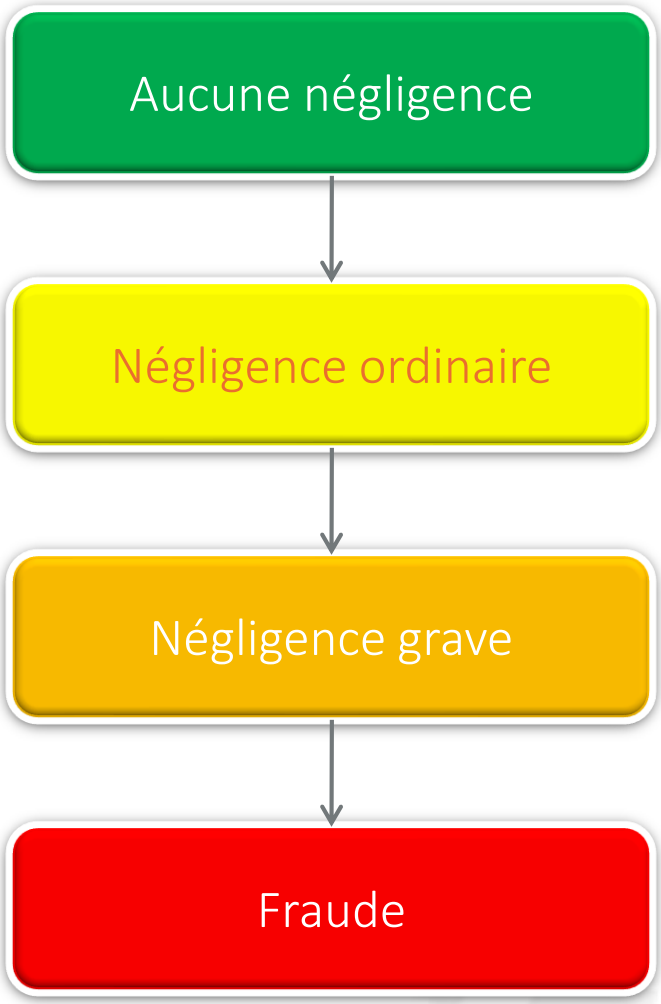
Conscience professionnelle 4C

Confidentialité 4D

Indépendance 4E

Approche fondée sur la preuve 4F

Responsabilité des auditeurs



Points d'attention

phosforea
my learning experience

Gestion de conflits avec l'audité

Conflit interne

Manque de coopération /antagonisme

Entrevue inefficace

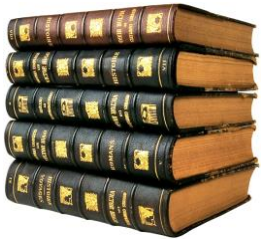
Temps gaspillé

phosforea
my learning experience

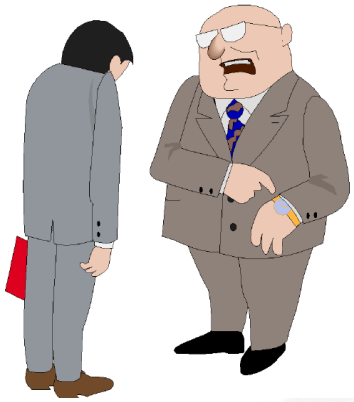
Gestion de conflits entre les auditeurs

Divergence d'opinions

Conflit personnel



Différence de méthodes de travail



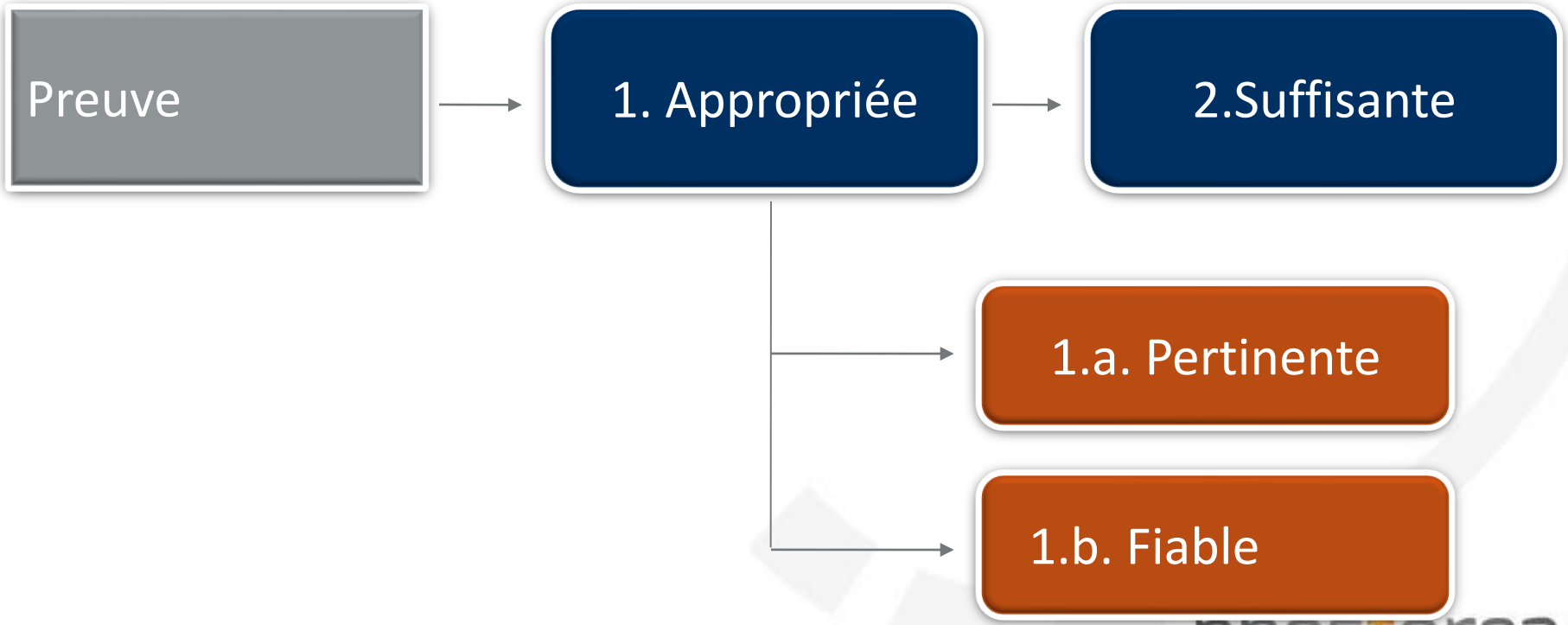
Attitude au travail

phosforea
my learning experience

La preuve

Qualité de la preuve de l'audit

Une preuve doit être compétente, puis suffisante

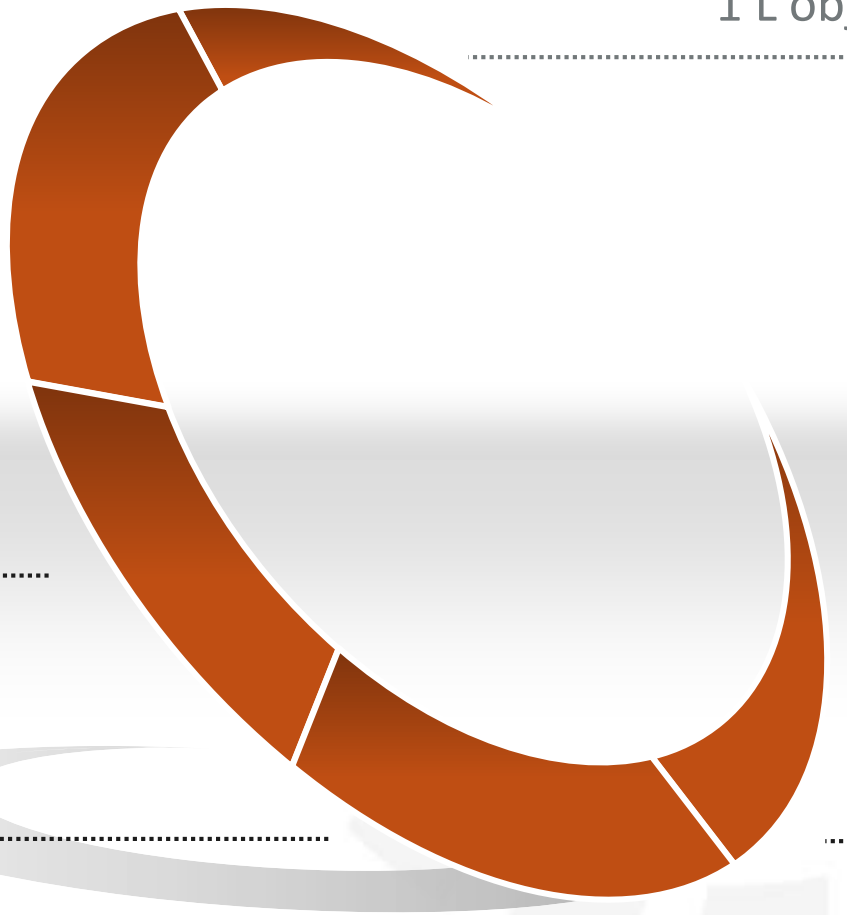


Fiabilité d'une preuve d'audit

- Principaux déterminants

1 L'objectivité de la preuve

2. Le Moment (timing) de la preuve



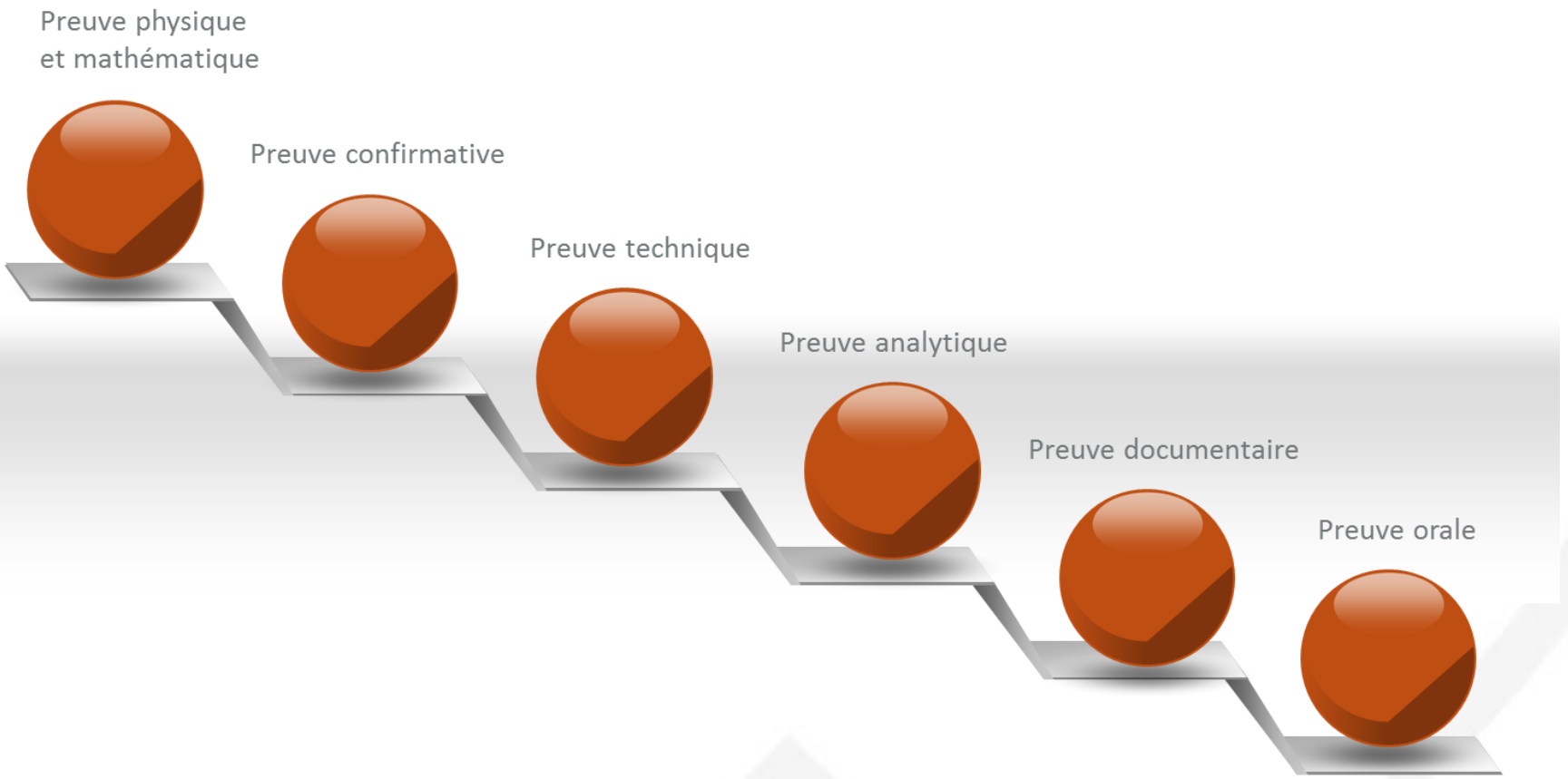
3. L'indépendance de la source

4. La collecte de la preuve

5. Le système de contrôle interne

phosforea
my learning experience

Fiabilité de la preuve dans l'audit



phosforea
my learning experience

Exercice

Quelle preuve pour ?

Donnez au moins deux éléments de preuve pour :

- Politique de Sécurité : existence et connaissance de la PSSI
- Processus de gestion des actifs : marquage de tous les actifs selon leur niveau de classification
- Vidéo-Surveillance : existence de video-surveillance à l'intérieur d'un bâtiment
- Enregistrements : production de traces horodatées pour les équipements réseaux

Constats d'audits

phosforea
my learning experience

Constatations d'audit - définition

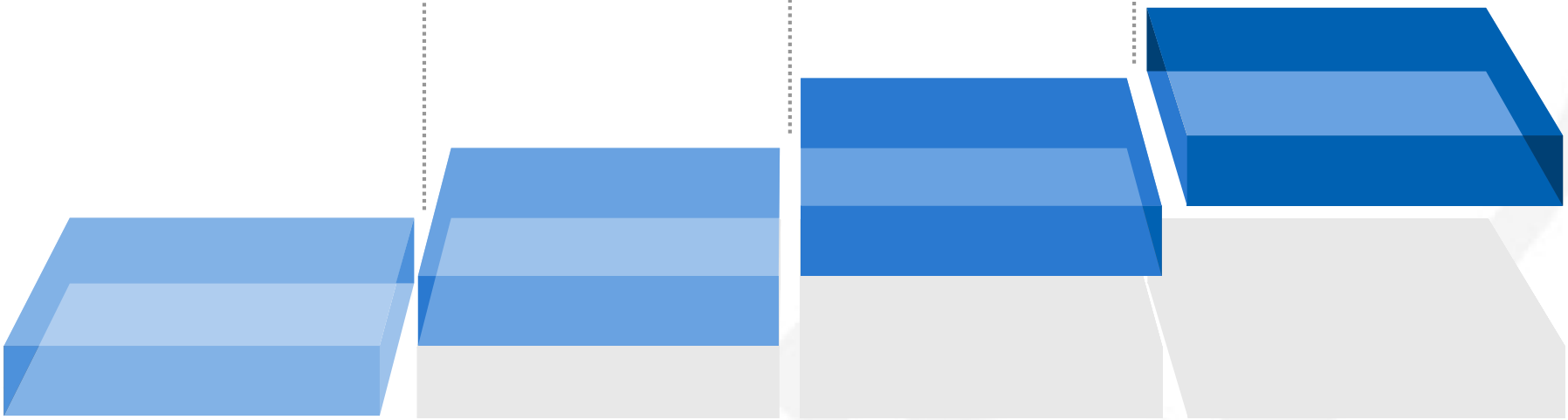
- ISO 19011, Clause 3.4

Constatations d'audit

- Résultats de l'évaluation des preuves d'audit par rapport aux critères d'audit
- Note : Les constatations d'audit indiquent la conformité, la non-conformité ou l'identification des opportunités d'amélioration

Constatations d'audit

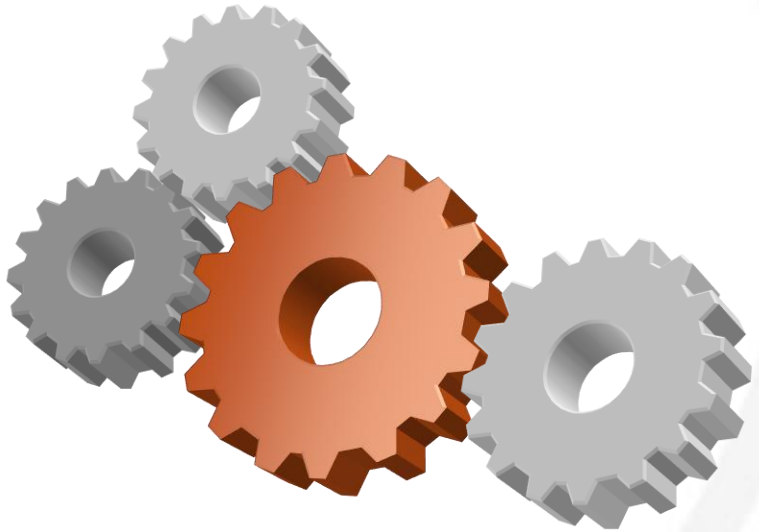
Conformité	Observation	Non-conformité mineure	Non-conformité majeure
Situation dans laquelle toutes les exigences ont été satisfaites	Situation ou élément noté durant l'audit pouvant être l'objet d'une amélioration continue sans constituer pour autant une non-conformité	Situation dans laquelle un aspect de la conformité à une exigence n'a pas été rempli	Absence de conformité à une exigence requise ou échec total de son efficacité



phosforea
my learning experience

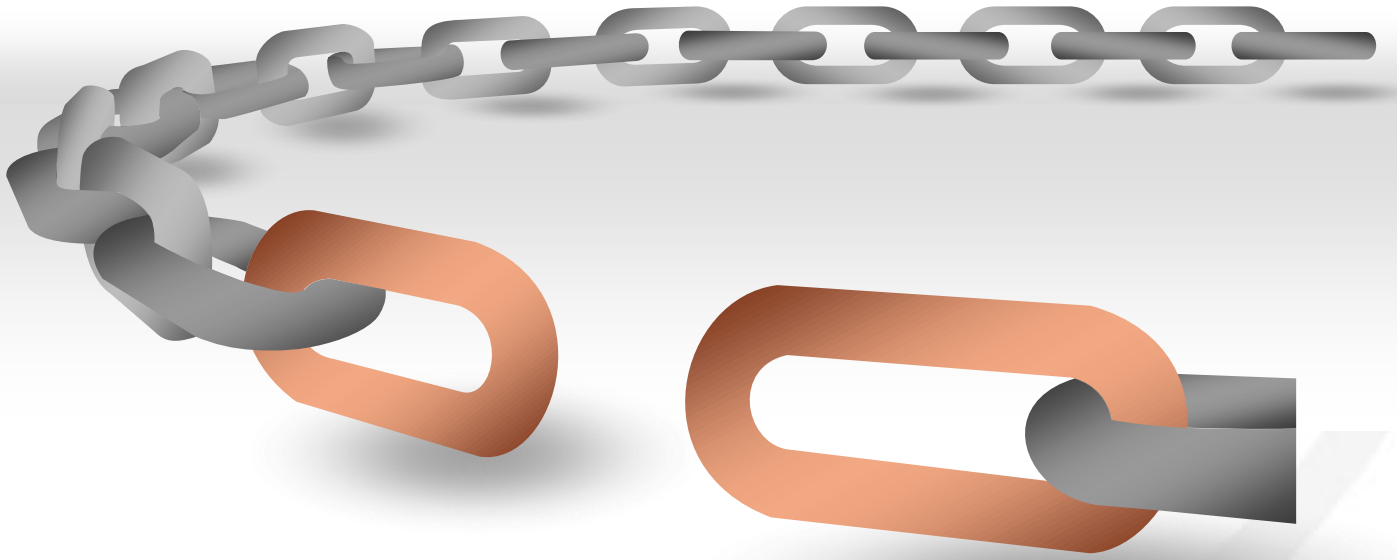
Observation

- **Définition :** Une observation est une situation ou un élément noté durant l'audit pouvant être l'objet d'une amélioration continue sans constituer une non-conformité
- Les observations sont souvent associées à des recommandations pour améliorer l'efficacité du système de management
- L'audité n'a aucune obligation de mettre en œuvre des actions correctives suite à des observations de l'auditeur



Anomalie

Définition: Une anomalie est une déviation accidentelle ou isolée d'une exigence. C'est une déviance par apport aux cibles établies par l'organisme, mais qui demeure dans des valeurs établies et acceptées (seuil acceptable)



Important : Ne constitue pas nécessairement une non-conformité

Non-conformité mineure

- Une situation dans laquelle un aspect de la mise en œuvre ou de l'application d'une mesure n'a pas été rempli :

  - telle qu'elle soulève **certains doutes** quant à l'adéquation du système à protéger la confidentialité, l'intégrité, ou la disponibilité des informations sensibles

  - et/ou que cela présente un **risque mineur mais non négligeable** qui pourrait être perçu par les parties prenantes de l'organisme

Non-conformité majeure

- Absence d'une mesure requise ou échec total de son efficacité :
  - Telle qu'elle soulève des **doutes significatifs** quant à l'adéquation du système à protéger la confidentialité, l'intégrité ou la disponibilité des informations sensibles
  - et/ou que cela représente un **risque inacceptable** qui pourrait être perçu par les parties prenantes de l'organisme

Rédaction des constats d'audit

- Équilibre entre les preuves et les critères

Constats d'audit

Preuves

Critères

phosforea
my learning experience

Rapport de non-conformité

- Si un constat d'audit est une non-conformité, l'auditeur doit le documenter dans un rapport de non-conformité
- Il y a 3 éléments pour bien documenter une non-conformité :
    1. Description de la non-conformité observée (la preuve appuyant les constats)
    2. Description des exigences pour lesquelles la non-conformité a été détectée (les critères de l'audit)
    3. Rapport de non-conformité (mineure ou majeure)

Rapport de non-conformité

RAPPORT DE NON-CONFORMITÉ		
No. de non-conformité : 3	**Client :** Thalia Technologies	**N° dossier :** 34527
Processus : Gestion des actifs	**Numéro de clause :** A.8.1.1.	**Site :** Montréal
Critères d'audit : Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré		
Description de la non-conformité observée : Sur un échantillon de 25 actifs analysés venant de la liste des actifs, seulement 5 actifs étaient correctement identifiés. **Recommandation :** Établir un inventaire de tous les actifs importants et identifier clairement les actifs en incluant, par exemple : le type, son propriétaire, son format, son emplacement, les informations relatives à sa sauvegarde et à la licence ainsi que sa valeur pour l'organisme.		
Auditeur : R. St-Germain **Date :** 5 juin 2007	**Reconnaissance du représentant audité :** non-conformité présentée à Monsieur R. Smith et confirmée le 3 juin 2007	**Non-conformité** Majeure* Mineure*

phosforea
my learning experience

Bénéfice du doute

- Bénéfice du doute et non-conformité
- Le but d'un audit est de vérifier la conformité, et non pas de chercher des non-conformités
- S'il n'y a pas de preuve de non-conformité
  - Il n'y a pas de non-conformité
- S'il y a une preuve de non-conformité
  - On doit documenter une non-conformité

Critères Communs

Evaluation par la confiance

phosforea
my learning experience

Les Critères Communs

- Norme ISO
  - ISO/IEC 15408-1:2009 : Introduction et modèle général
  - ISO/IEC 15408-2:2008 : Composants fonctionnels de sécurité
  - ISO/IEC 15408-3:2008 : Composants d'assurance de sécurité

- L'objectif étant de déterminer un « degré de confiance » de produits & systèmes de sécurité
  - Par l'analyse et le test des fonctions de sécurité d'un produit
  - Par l'analyse et le test des processus de conception & développement

- Emission d'un « certificat » attestant que les produits certifiés sont conformes à une spécification technique appelée « cible de sécurité »

Les critères Communs

- Différents niveaux de prise en compte du standard
  - Pays habilités à délivrer un certificat
  - Pays reconnaissant les certificats sans pouvoir en émettre

- le décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits des technologies de l'information décrit le schéma de certification français

- L'ANSSI est chargée d'instruire les certifications, en s'appuyant sur les travaux d'évaluation réalisés par des laboratoires agréés (premier ministre) et accrédités (COFRAC)

Centres d'Evaluation agréés

- Les CESTI réalisent les évaluations, agissant en tant que tierce partie indépendante des développeurs du produit et du commanditaire.
- Les activités de CESTI doivent être cloisonnées vis-à-vis des autres activités de l'organisme auquel il est rattaché
- Obligation d'impartialité et d'indépendance

- Produits logiciels et équipements réseaux
  - AMOSSYS, OPPIDA, SOGETI
- Produits composants électroniques, microélectroniques et logiciels embarqués
  - CEA-LETI, SERMA, THALES
- Produits équipements matériels avec boitiers sécurisés
  - CEA-LTI, THALES, AMOSSYS+SERMA, OPPIDA+SERMA

Différents référentiels

Un **produit (ou TOE)** est certifié conforme par rapport à

Une **Cible de Sécurité (ST)**, elle-même certifiée conforme à un cahier des charge appelé

Profil de Protection (PP), qui est un ensemble d'exigences haut niveau, partagé par une communauté et établi sur la basse

Des normes ISO 15408

Les Profils de Protection

- Standards fonctionnels :
  - décrivent un ensemble d'exigences et objectifs de sécurité
  - A intégrer dans un produit ou un système
  - Selon les besoins d'utilisateurs/consommateurs

- Exigences et objectifs
  - indépendants de toute implémentation
  - Réutilisables/génériques

- Décrit la TOE !

Cibles de Sécurité

- Spécification du besoin de sécurité : exigences de sécurité détaillées

- Spécifications techniques des fonctions de sécurité décrites dans le PP
- Présente les menaces qui pèsent sur les objectifs
- Spécifie les mécanismes de sécurité qui seront employés

- Une ST peut se déclarer conforme à une ou plusieurs PP

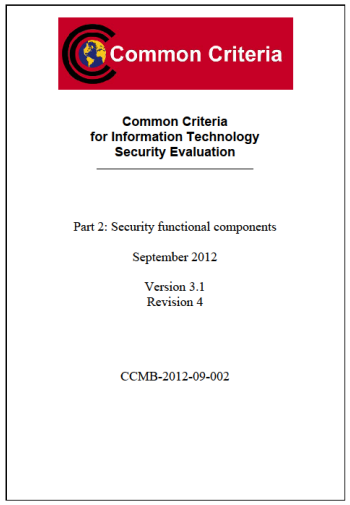
Cible d'évaluation (TOE)

- Produit ou système, et sa documentation, soumis à une évaluation de la sécurité

- La description de la TOE se doit de décrire ses ressources (ce qui est utilisé et/ou consommé dans la TOE) et les fonctions de sécurité traitées
  - TOE Security Functions = TSF

Composant fonctionnels de Sécurité

- Catalogue de composants fonctionnels de sécurité classifiés
  - En classes
  - Puis en familles
  - Puis en composants


Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 2: Security functional components

September 2012

Version 3.1
Revision 4

CCMB-2012-09-002

Classe	Nom
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentification
FMT	Security Management
FDR	Privacy
FPT	Protection of the TSF
FRU	Ressource Utilisation
FTA	TOE Access
FTP	Trusted Path/channels

Exemple de classe : FTA

Famille	Description
FTA_LSA	Limitation of scope of selectable attributes
FTA_MCS	Limitation on multiple conccurent sessions
FTA_SSL	Session locking and termination
FTA_TAB	TOA Access banners
FTA_TAH	TOE Access history
FTA_TSE	TOE Session establishment

Composant	Description
FTA_MCS.1	Basic limitation on multiple concurrent sessions - The PP/ST author should specify the default number of maximum concurrent sessions to be used
FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions - The PP/ST author should specify the rules that determine the maximum number of concurrent sessions - The PP/ST author should specify the default number of maximum concurrent session to be used

Composant d'assurance de Sécurité

- Exigences pour le développeur
- Tâches à réaliser pour l'évaluateur

Class	Description
API	Protection Profile Evaluation
ASE	Security Target Evaluation
ADV	Development
AGD	Guidance Documents
ALC	Life-Cycle Support
ATE	Tests
AVA	Vulnerability Assessment
ACO	Composition

LVL	Description
AVA_VAN.1	Vulnerability Survey
AVA_VAN.2	Vulnerability Analysis
AVA_VAN.3	Focused Vulnerability Analysis
AVA_VAN.4	Methodical Vulnerability Analysis
AVA_VAN.5	Advanced Methodical Vulnerabilty Analysis

Req	Description
AVA_VAN.1.1D	The developper shall provide the TOE for testing
AVA_VAN.1.1C	The TOE shall be suitable for testing
…	
AVA_VAN.1.3E	The valuator shall conduct penetration testing, based on […]

phosforea
my learning experience

Niveaux d'Assurance

Ref.	Niveau d'assurance
EAL1	Testé fonctionnellement
EAL2	Testé structurellement
EAL3	Testé et vérifié méthodiquement
EAL4	Conçu, Testé et vérifié méthodiquement
EAL5	Conçu de façon semi-formelle et testé
EAL6	Conception vérifiée de façon semi-formelle et système testé
EAL7	Conception vérifiée de façon formelle et système testé

Approche d'évaluation

- A partir de la cible de sécurité
  - Accord entre le développeur, les clients, les évaluateurs et l'autorité de certification
- La ST contient :
  - Description de la TOE
  - Exigences fonctionnelles et assurances de TOE
  - Exigences d'environnement
  - Résumé des spécifications de TOE
  - Environnement sécurité de TOE
  - Déclarations PP
  - Logique/Démonstration

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Fin du module

Ce module est à présent terminé, vous pouvez retourner sur votre tableau de bord.

phosforea
my learning experience