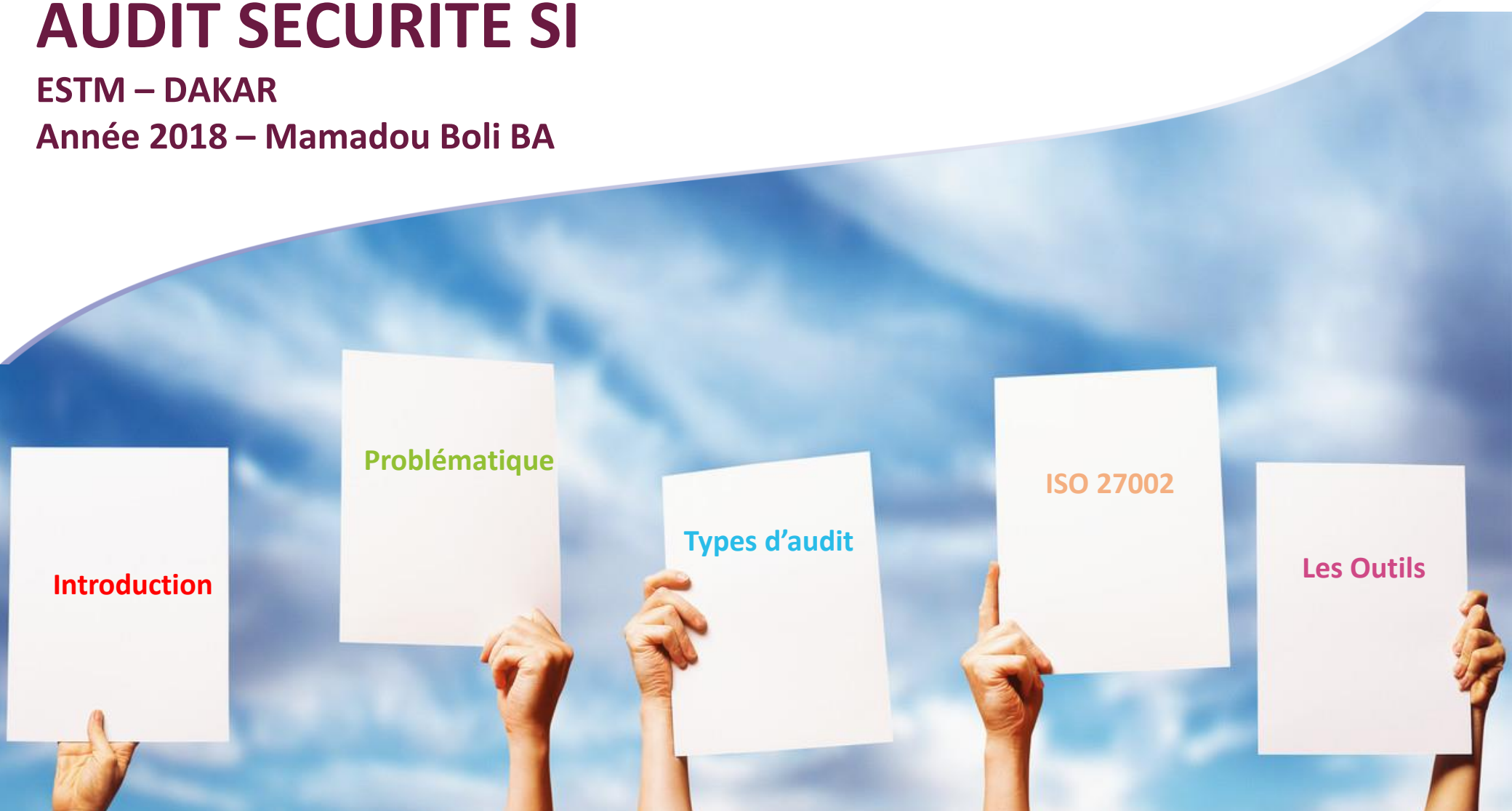
AUDIT SECURITE SI

ESTM – DAKAR

Année 2018 – Mamadou Boli BA

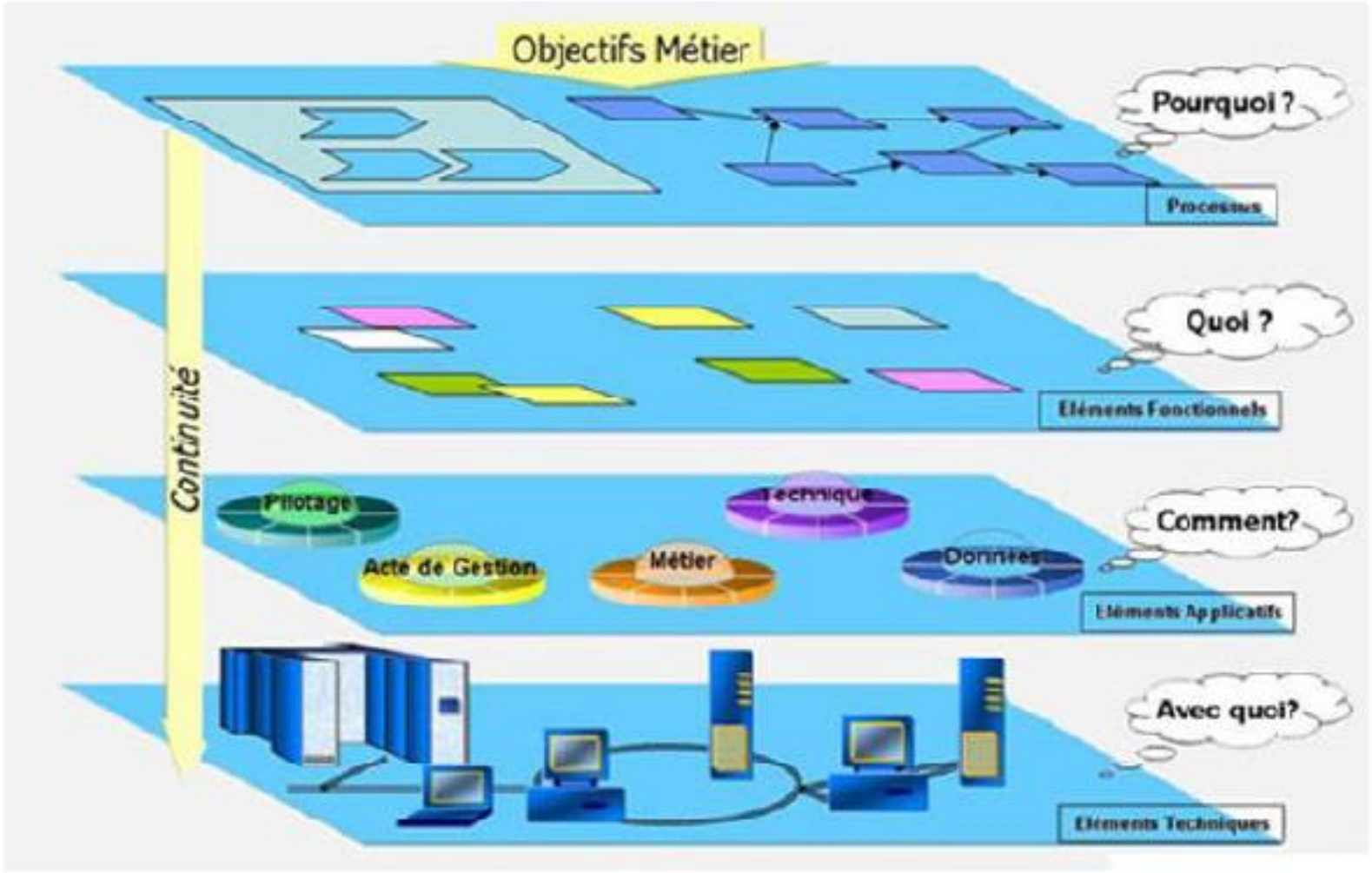


Sommaire

1. Introduction
2. Problématique
3. Types d’audit
4. ISO 27002
5. Les outils

Introduction

Définition



Introduction

Définition

- Pour la sécurité du SI, un ensemble de mesures de sécurité organisationnelles, procédurales ou techniques doivent être mise en œuvre sur l'ensemble des moyens supportant le système d'information.

- L'objectif de ces mesures de sécurité est

La confidentialité

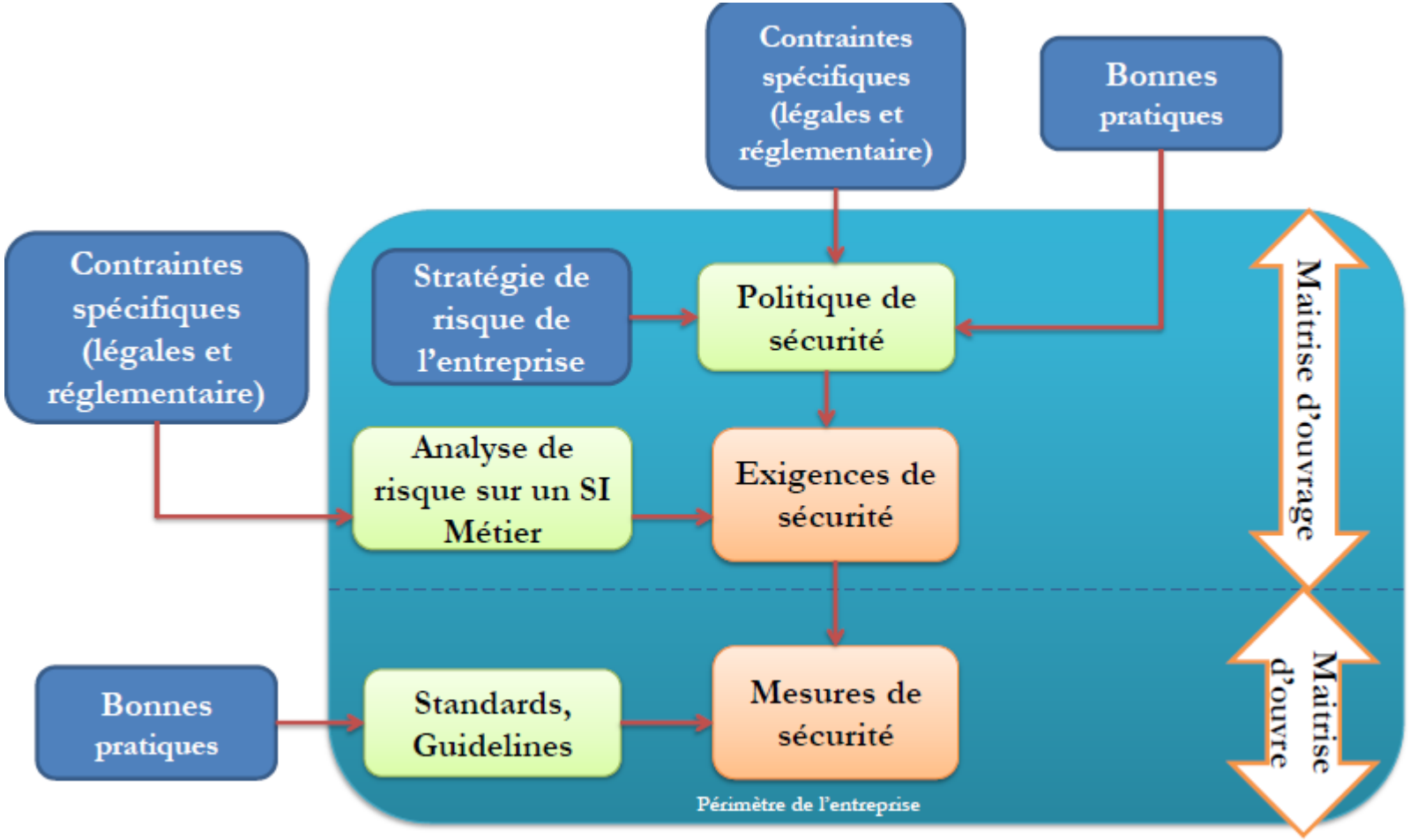
L'intégrité

La disponibilité

La traçabilité

Problématique

Schéma



Problématique

Piste de vérification

- Les questions auxquelles doivent répondre les audits de sécurité du SI

A quelles exigences légales et réglementaires le Système d'Information est	il soumis ?
Ces contraintes légales et réglementaires sont	elles respectées ?
La politique de sécurité est	elle alignée sur la stratégie d'entreprise ?
L'organisation de la sécurité est	elle fonctionnelle ?
Les objectifs et contrôles de sécurité sont	ils exhaustifs?
La continuité des activités de l'entreprise est	elle assurée ?
Les mesures de sécurité opérationnelles sont	elles alignées sur la politique de sécurité ?
Les mesures de sécurité opérationnelles mises en place sont	elles efficaces ?

Les types d'audit de sécurité

Les différents types

- Audit de la politique de sécurité

Adéquation de la politique de sécurité à la stratégie de risques de l'entreprise, aux contraintes légales et réglementaires et aux bonnes pratiques

- Audit de la mise en œuvre de la politique de sécurité

Respect des exigences de sécurité au sein de l'entreprise au travers de la mise en œuvre de mesures de sécurité adéquates et pérennes,

- Audit de la prise en compte de la sécurité dans un projet

- Audit de l'efficacité des mesures de sécurité

Test d'intrusion, audit de vulnérabilité sur l'ensemble des composantes du SI

- Audit réglementaire

Les types d'audit de sécurité

Les référentiels

Audit de sécurité	Référentiel
Audit de la politique de sécurité Adéquation de la politique de sécurité à la stratégie de risques de l'entreprise, aux contraintes légales et réglementaires et aux bonnes pratiques,	Contexte légale et réglementaire, Stratégie de risque de l'entreprise, ISO 27002.
Audit de la mise en œuvre de la politique de sécurité Respect des exigences de sécurité au sein de l'entreprise au travers de la mise en œuvre de mesures de sécurité adéquates et pérennes	Politique de sécurité de l'entreprise, ISO 27002, CoBIT ITIL ISO 20000
Audit de l'efficacité des mesures de sécurité	OWASP (Open Web Application Security Project), Information Security Web sites, Bases de vulnérabilités.
Audit réglementaire	ISO 27002 Référentiel de l'ANSI

Les types d'audit de sécurité

Typologies

- **L'audit de la politique de sécurité** doit permettre de s'assurer de la pertinence de celle-ci compte tenu de la stratégie de risques de l'entreprise, du contexte légale et réglementaire ainsi que des bonnes pratiques.
  - Le terme « politique de sécurité » peut recouvrir
    - ✓ la politique de sécurité du groupe,
    - ✓ la déclinaison de la politique de sécurité du groupe au niveau des différentes entités ou métiers
    - ✓ l'ensemble des politiques de sécurité détaillées couvrant les domaines comme le contrôle d'accès, la continuité, la classification de l'information, la protection antivirale …
- **L'audit peut également couvrir :**
  - la méthodologie d'analyse de risques mise en œuvre
  - des standards et procédures qui découlent de la politique de sécurité

L'APPROCHE REPOSE SUR DES INTERVIEWS ET DES ANALYSES DOCUMENTAIRES

Les types d'audit de sécurité

Typologies

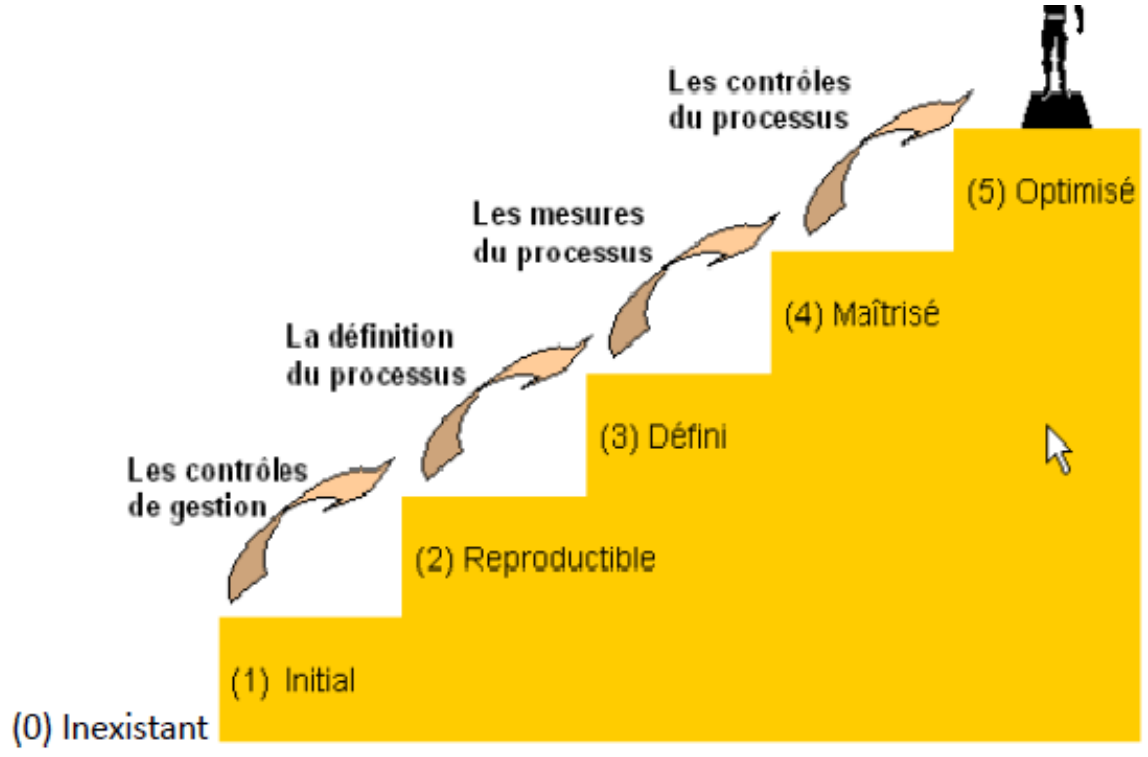
- **L'audit de la mise en œuvre de la politique de sécurité** doit permettre de s'assurer que les exigences de sécurité sont satisfaites au travers de la mise en œuvre de mesures de sécurité.
- Les grilles d'investigation sont construites sur la base de la politique de sécurité et/ou de l'ISO 27002 et/ou de Cobit.
- Les grilles d'investigation spécifiques sont construites pour approfondir des thématiques comme les solutions antivirus, les dispositifs correctifs de sécurité et anti-spam, le plan de secours et de continuité …

L'approche repose sur des interviews, des visites de sites, des analyses documentaires et des revues de paramétrage.

Les types d'audit de sécurité

Typologies

- Pour chaque domaine de la grille d'investigation ISO 27002, les processus sont répartis en six niveaux de maturité qu'une organisation va gravir en fonction de la qualité des processus qu'elle a mis en œuvre.



Les types d'audit de sécurité

Typologies – les niveaux de maturité de ISO 27002

0 - Aucun - processus/documentation en place

1 - Initial - Le processus est caractérisé par la prédominance d'interventions ponctuelles, voire chaotiques. Il est très peu défini et la réussite dépend de l'effort individuel

2 - Reproductible - Une gestion élémentaire de la sécurité est définie pour assurer le suivi des coûts, des délais et de la fonctionnalité. L'expertise nécessaire au processus est en place pour reproduire la même action

3 - Défini - Le processus de sécurité est documenté, normalisé et intégré dans le processus standard de l'organisation

4 - Maîtrisé - Des mesures détaillées sont prises en ce qui concerne le déroulement du processus et la qualité générée. Le processus et le niveau de qualité sont connus et contrôlés quantitativement

5 - Optimisation - Une amélioration continue du processus est mise en œuvre par une rétroaction quantitative émanant du processus lui-même et par l'application d'idées et de technologies innovatrices

Les types d'audit de sécurité

Typologies – Audit des composants du SI

- Chaque composant du SI doit disposer d'une grille d'évaluation pour approfondir la dimension technique de l'audit sécurité

Audit de la connexion Internet

Audit des accès distants

Audit des serveurs et des postes de travail

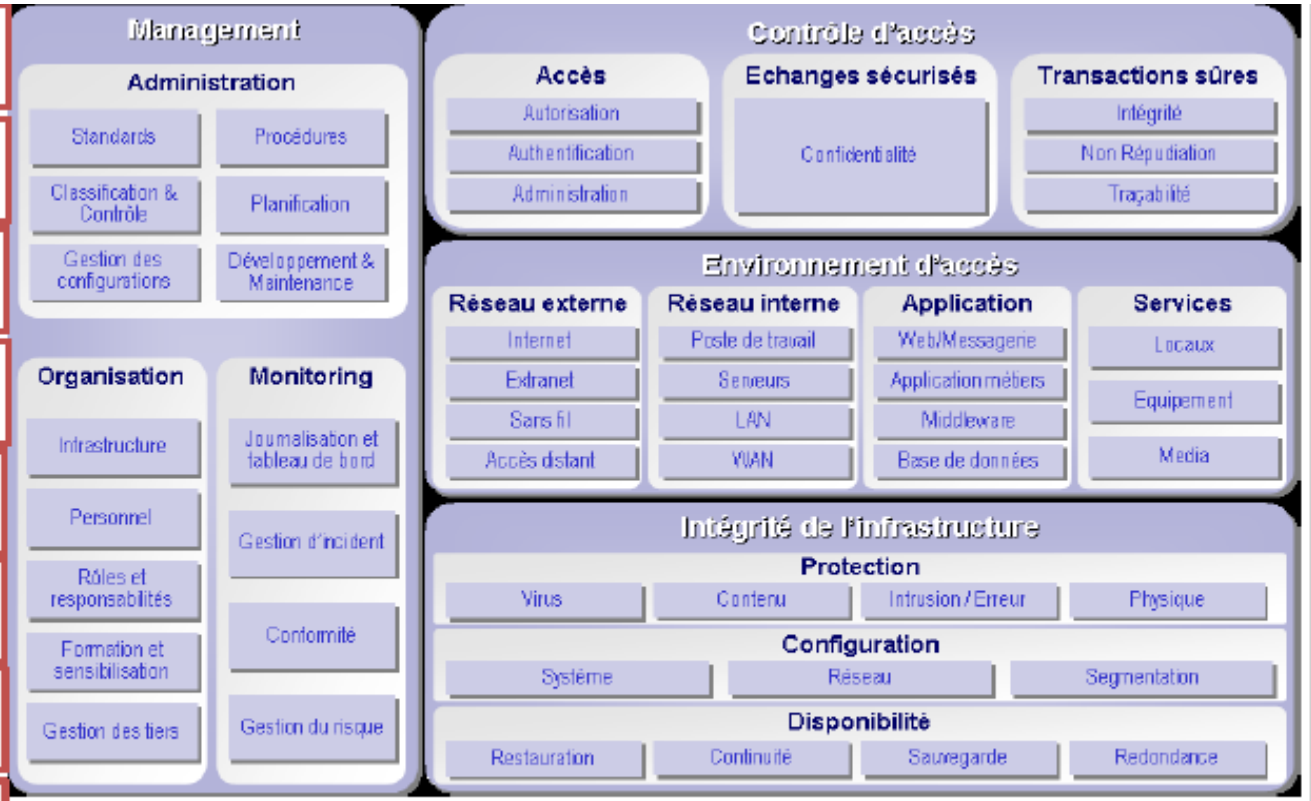
Audit des équip. de réseau & sécurité

Audit de la solution Antivirale

Audit de la Gestion des Tiers

Audit de Gestion d'Incident

Revue du plan de continuité



Les types d'audit de sécurité

Typologies – Audit de l'efficacité des mesures de sécurité

- **Tests d'Intrusion**

Pour s'assurer de la sécurité de l'Infrastructure face à des scénarii d'attaques de personnes malveillantes (pirate, prestataire, ex-employé, utilisateur interne …)

- **Audit de sécurité technique**

Pour déterminer si les firewalls, serveurs web, routeurs, connexions distantes, connexion sans fils, applications, sont configurés et mis en œuvre de manière adéquate au regard des risques encourus

Les types d'audit de sécurité

Typologies – Audit de l'efficacité des mesures de sécurité

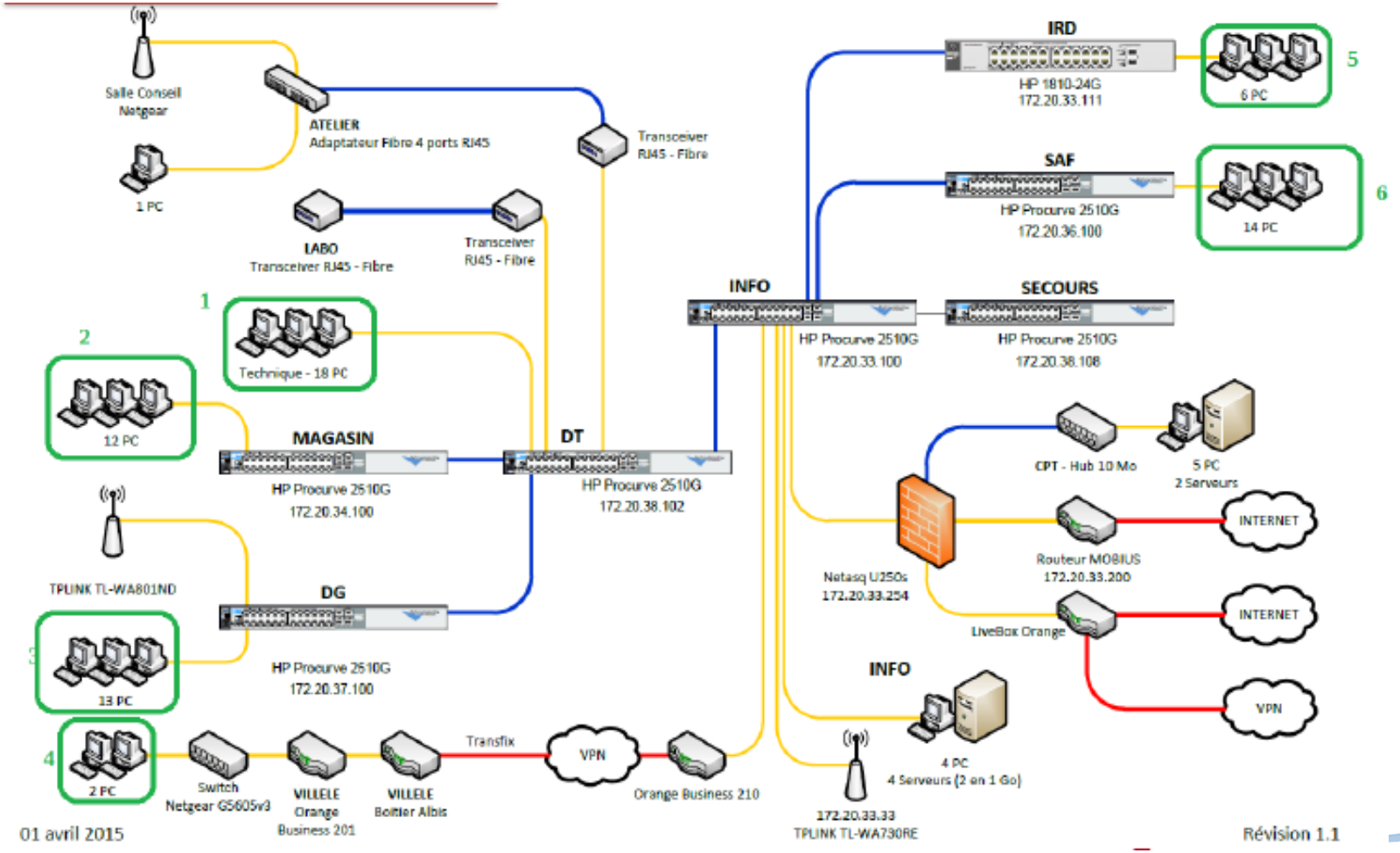
- **Tests d'Intrusion**

Tests d'Intrusion
Externe
Interne
Physique
Intranet
Extranet
Wifi
Accès à distance

Les types d'audit de sécurité

Typologies – Audit de l'efficacité des mesures de sécurité

- **Audit de la sécurité technique**



ISO 27002

Les Domaines

Domaines de sécurité de l'information (niveau 1)
La norme ISO/IEC 27002:2013 recense de nombreux objectifs de contrôle répartis dans chacun des 14 domaines

Catégories de sécurité (niveau 2)

- La structure de la norme est semblable pour chacune des 35 catégories de sécurité :
  - Un objectif de contrôle qui fait l'état sur ce qui doit être appliqué est énoncé,
  - Un ou plusieurs contrôles à appliquer sont proposés pour remplir l'objectif de contrôle de la catégorie de sécurité

Contrôles (niveau 3)
Au niveau inférieur, la structure de la norme est semblable pour chacun des 114 objectifs de contrôle qui ont été définis :
Control : le contrôle permet de définir précisément l'état pour satisfaire à l'objectif de contrôle,
Implementation guidance : le guide d'implémentation propose les informations détaillées pour permettre d'effectuer l'implémentation du contrôle et de satisfaire à l'objectif de contrôle.
Other information

5. Politiques de sécurité de l'information
6. Organisation de la sécurité de l'information
7. Sécurité des ressources humaines
8. Gestion des actifs
9. Contrôle d'accès
10. Cryptographie
11. Sécurité physique et environnementale
12. Sécurité liée à l'exploitation
13. Sécurité des communications
14. Acquisition, développement et maintenance des systèmes d'information
15. Relations avec les fournisseurs
16. Gestion des incidents liés à la sécurité de l'information
17. Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
18. Conformité

Les Outils

Référentiel de la politique de sécurité établi par l'ANSI

- **Repose sur 38 critères regroupés en 11 domaines:**
  - D1. Leadership et gouvernance de la sécurité
  - D2. Gestion des risques liés à la sécurité du système d'information
  - D3. Sécurité des actifs
  - D4. Sécurité du personnel et développement des capacités
  - D5. Protection de l'environnement physique du système d'information
  - D6. Sécurité des services d'infrastructure
  - D7. Sécurité des services métiers
  - D8. Sécurité des terminaux
  - D9. Sécurité des applications
  - D10. Gestion des incidents de sécurité
  - D11. Gestion de la continuité des activités

Les Outils

Référentiel de la politique de sécurité établi par l'ANSI

Exemple

➢ **D2. Gestion des risques liés à la sécurité du système d'information**

Critères d'audit:

(7) L'audité doit maintenir un système de gestion des risques de sécurité des systèmes d'information

Vérifications à effectuer:

- Si l'audité a identifié et documenté les risques de sécurité du SI auxquels il est exposé,
- Si le niveau de risque a été quantifié,
- Si, pour chaque risque considéré comme inacceptable, des mesures ont été prises pour ramener le risque à un niveau acceptable,
- Si un suivi permanent des risques et de leurs niveaux a été mis en place,
- Si chaque risque, pris individuellement, a été pris en charge et a fait l'objet d'une décision de traitement (Acceptation, Transfert, Réduction, Evitement).

Preuves suffisantes d'audit:

- Document de cartographie des risques répertoriés
- Document de traitement des risques (Plan d'action, etc.)

Les Outils

Modèle de rapport

- Champ de l'audit,
- Méthodologie d'audit,
- Synthèse des résultats de l'audit,
- Présentation détaillée des résultats de l'audit,
- Appréciation des risques,
- Plan d'action,
- Annexes
  - Description du SI de l'organisme
  - Planning d'exécution réel de la mission d'audit de la sécurité du SI
  - Evaluation de l'application du dernier plan d'action
  - Etat de maturité de la sécurité du SI
  - Plan d'action proposé

Les Outils

Contenu du rapport

Pour qui ?
- Direction Générale,
- Audit interne,
- Métier,
- Maison mère,
- Organisme certificateur …

Sur quel périmètre ?
- Organisation,
- Site,
- Service,
- Environnement technique,
- Application, …

Par qui ?
- Interne / externe

Selon quel référentiel ?
- Lois et règlements
- Organisme
- Bonnes pratiques (ISO,…)

Dans quel but ?
- Alignement de la politique de sécurité sur la stratégie d'entreprise,
- Conformité aux lois et règlements,
- Efficacité et efficience des contrôles,
- SOX, contrôle interne,
- Identification des risques auxquels est exposé le SI…

De quelle nature ?
- Audit de la politique de sécurité,
- Audit de la mise en œuvre de la politique de sécurité,
- Audit de l'efficacité des mesures de sécurité.