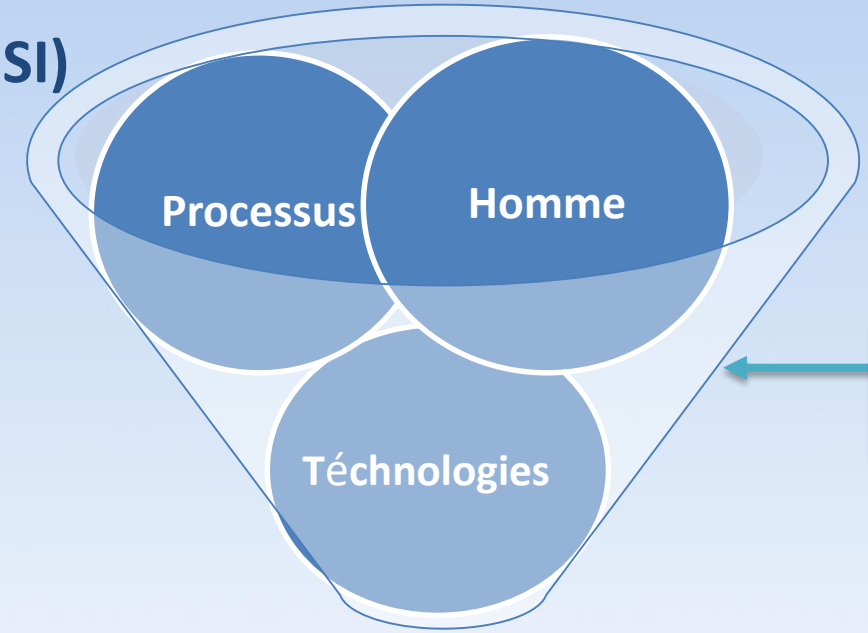
Security Audits of Information Systems

Presented by: **NJEI CHECK**
Eng, PMP, COBIT, ITIL;
Security Audit / e-Gov Expert, ANTIC
Email: njei.check@antic.cm

SUMMARY

Introduction

Système d'information (SI)



Cadre Règlementaire & Juridique

?

Sécurité

- ❖Disponibilité
- ❖Confidentialité
- ❖Intégrité

Introduction

Audit de sécurité du SI:

Processus systématique, indépendant et documenté permettant de recueillir des informations objectives pour déterminer dans quelle mesure les éléments du système d'information satisfont aux exigences des référentiels, standards et bonnes pratiques en matière de sécurité des SI.

Introduction

- ***Vulnérabilité:***

  Caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information

- ***Menace:***

  Cause potentielle d'incident, qui peut résulter en un dommage sur le système d'information

- ***Risque:***

  Résultante de l'exploitation d'une ou plusieurs vulnérabilités par une menace

Référentiel
(ISO 27001/27002)

Organizational

- information security policy
- organization of information security
- asset management
- human resources security
- Supplier relationships
- Compliance

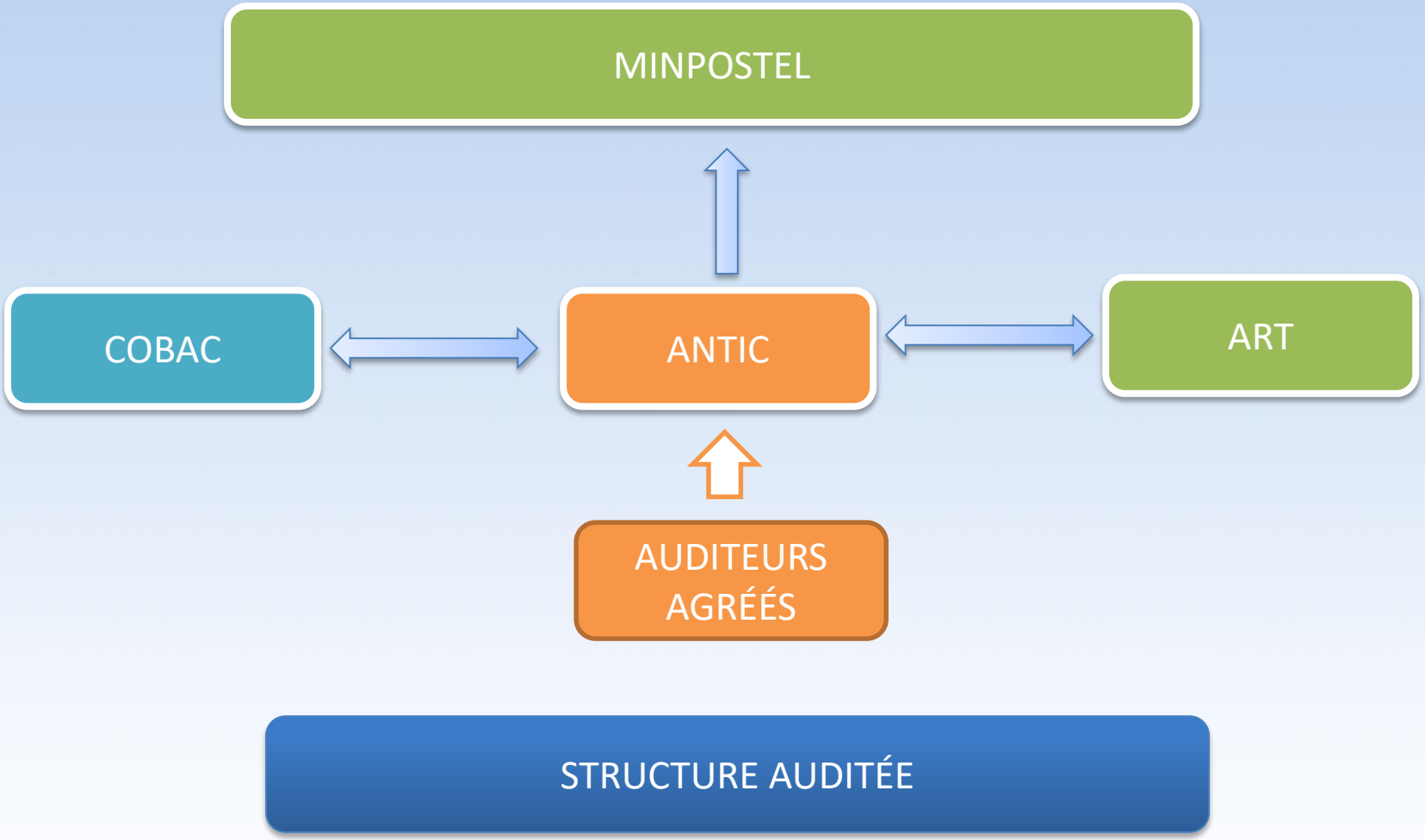
Physical

- physical and environmental security

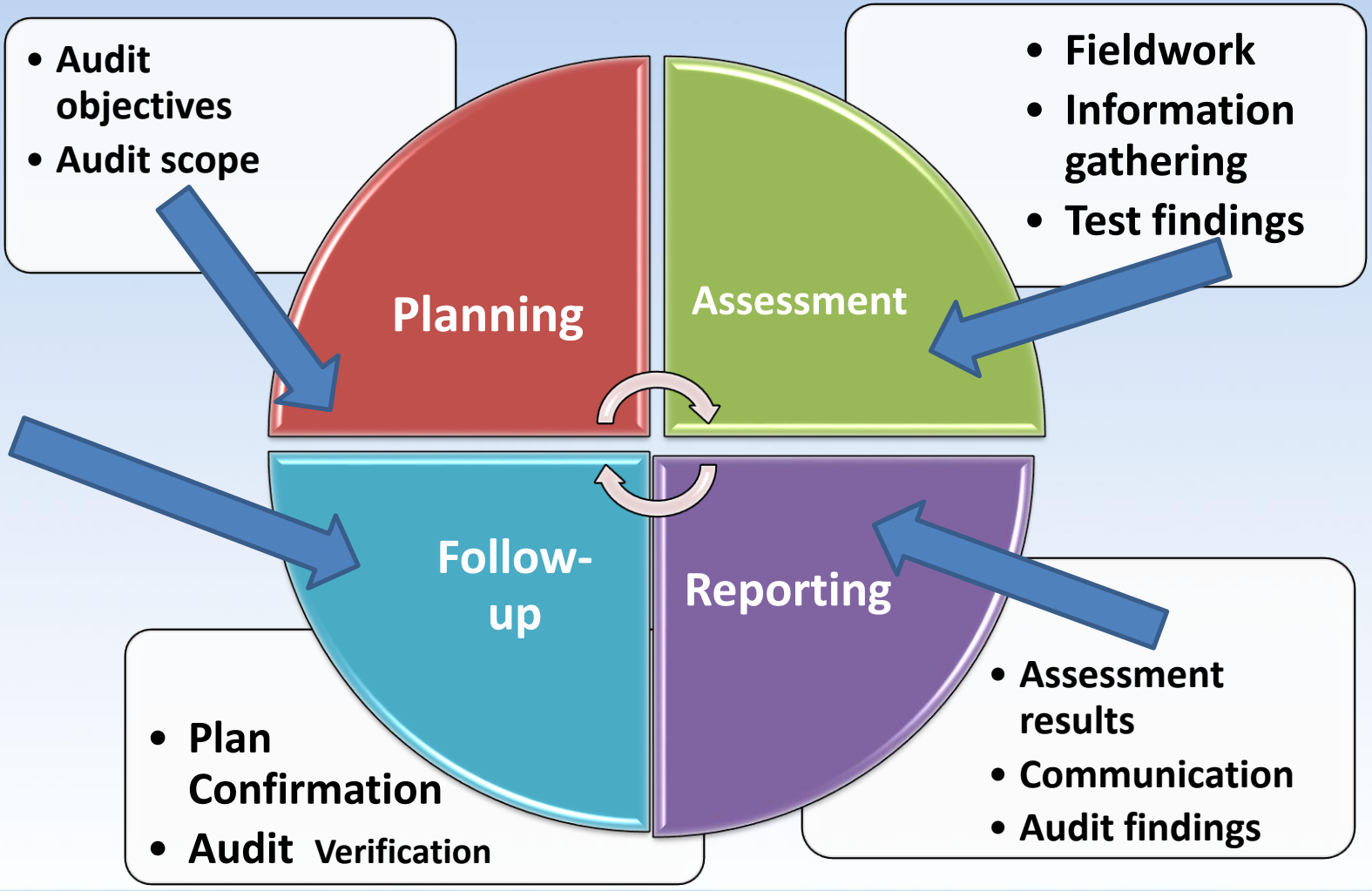
Technical

- access control
- communications security
- information security incident management
- operations security
- information systems acquisition, development and maintenance
- cryptography
- Information security aspects of business continuity management

ACTEURS


MINPOSTEL
COBAC
ANTIC
ART
AUDITEURS AGRÉÉS
STRUCTURE AUDITÉE

Processus de la Réalisation des Audits



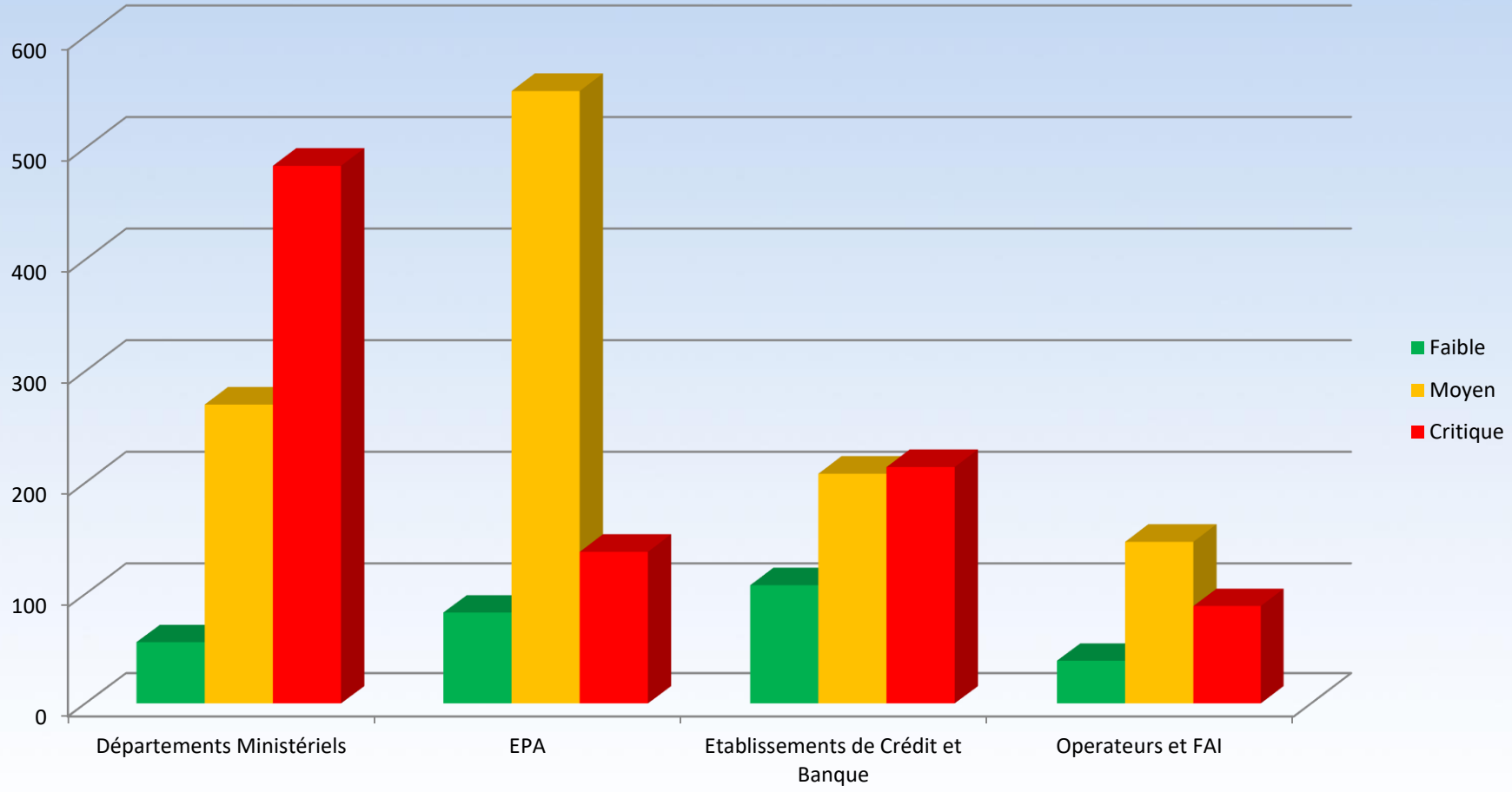
RESULTATS

Bilan de l'activité d'audit de sécurité par ANTIC depuis 2013

Année	Départements ministériels	Etablissements de crédit	EPA	Opérateurs de télécommunication et FAI	TOTAL
2013	14	4	1	4	**23**
2014	20	8	5	0	**33**
2015	1	4	1	3	**9**
2016	7	0	3	4	**14**
2017	10	0	8	8	**26**
2018	11	10	11	6	**38**
TOTAL	**62**	**26**	**29**	**25**	**143**

RESULTATS

Vulnérabilités identifiées (2013 – 2018) :14401



ENJEUX-> Un Cas

En 2017, **wannacry** est utilisé lors d'une cyber-attaque mondiale massive, touchant plus de 300 000 ordinateurs, dans plus de 150 pays en exploitant les versions antérieures à windows 10 n'ayant pas effectué les mises à jour de sécurité

RETOUR D'EXPÉRIENCE

- **Sur le plan Organisationnel**
  - Absence d'un **plan de gestion des risques** (Procédures, Méthodologie, cartographie des risques, Plan de traitement) ;
  - Absence de **Politique de sécurité du SI** ;
  - Absence de **guide/procédure de sécurisation des fichiers sensibles** ;
  - Absence de **classification des actifs** matériels et immatériels par niveau de criticité ;
  - Insuffisance de **Sensibilisation et de formation** du personnel sur la cybersécurité et les risques liés à l'utilisation des TIC;

RETOUR D'EXPÉRIENCE

- **Sur le plan Physique**
  - **Dispositifs de contrôle d'accès physiques** insuffisants ;
  - **Non-conformité des locaux techniques** (absence d'authentification double facteur, absence d'extincteurs, absence de journal d'accès, absence de détecteurs d'incendie et d'inondation, Absence de faux planchers, Câbles non étiquetés, Absence de portes coupe feu…);
  - **Non-conformité des salles des archives** (Absence d'un plan de classement, insalubrité, absence d'extincteur, absence de détecteurs d'incendie, non respect des standards,…).

RETOUR D'EXPÉRIENCE

- **Sur le plan Technique**
  - **Absence de mises à jour** et/ou de suivi des mises à jour des différents systèmes et composants utilisés ;
  - Absence d'une **politique de gestion des comptes maitres** ;
  - **Politique de gestion des mots de passe** pas toujours élaborée et/ou implémentée ;
  - Insuffisance dans la gestion et la **sécurisation des logs** ;
  - Inexistence d'une **table des autorisations** indiquant pour chaque personnel son profil, ses habilitations sur différents systèmes ;
  - Insuffisance dans la **sécurisation des sauvegardes** qui sont réalisées ;
  - Mauvaise **gestion des configurations** ;
  - Présence de nombreuses failles sur les **sites et applications web**

CONCLUSION

- Les actes cybercriminels, tout comme les atteintes à la sécurité de l'information ont un impact grave sur l'entreprise, notamment sur les aspects finances, conformité et réputation.
- Les audits de sécurité participent activement à maintenir un environnement sain, où les données sont collectées, traitées, stockées, transmises de façon sécurisée;
- Pour cette raison, chaque entreprise devrait procéder à un contrôle régulier du niveau de sécurité de son système d'information, ceci afin d'atteindre les objectifs stratégiques tout en préservant ses actifs les plus critiques;

THANKS FOR YOUR KEEN ATTENTION