الوكالة الوطنيّة للسّلامة المعلوماتيّة
National Agency for Computer Security

2ème workshop

Protection des infrastructures d'information critiques

Vision de l'ANSI

05 Décembre 2019

tunCERT
Tunisian Computer Emergency Response Team

AGENDA

- Etat des lieux
- Vision, orientations et objectifs
- Les défis

2

Trends 2019

trend #1: La cartocraphie du phishing est en train de changer, l'e-mail reste le 1er vecteur d'attaque

trend #2: Croissance de l'utilisation du mobile comme vecteur d'attaque

trend #3: Ciblage des gouvernements et des entreprises via des attaques par ransomware

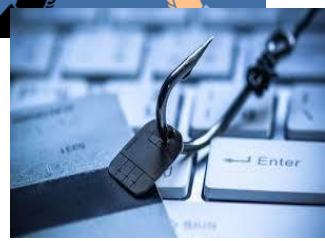
trend #4: Interêt à la protection des données à caractère personnel, à la souveraineté et à la conformité

trend #5: Croissance des investissements dans l'automatisation de la cybersécurité

Les prédictions pour 2020

1- Ransomwares ciblés
(Santé, Gouvernement, Industrial Control System)

2- Attaques par **Phishing** au delà des e-mails
(SMS, Plateforme de gaming, réseaux sociaux)



3- Montée des attaques **Mobile malware**

4- Croissance de l'activité de l'**assurance cybernétique**

5- Plus de **devices IoT**, plus de risques
(200 billion connected devices)

6- Explosion des données avec la **5G**

7- l'IA accélére la réponse aux attaques cybernétiques

Les mythes

Myth #3:
Je suis un “petit acteur” dans un “petit pays”, personne ne va me cibler.

Mythe #1:
Le système de production n’est pas connecté à internet, donc le risque n’est pas significatif

Myth #3:
Je suis protégé parce que j’utilise un protocole propriétaire
Mon système de production est protégé par défaut

Mythe #4:
Tout ce que j’ai besoin pour protéger mon système de production est d’installer un antimalware et un firewall

Mythe #5:
Les attaques cybernétiques liées au systèmes de production ne pourraient en aucun cas donner lieu à des pertes humaines ou des dommages physiques

Pourquoi protéger les IIC

- Complexité
- Mode distribué
- Interconnexion et Interdépendance
- Hétérogénéité
- Tendance à la hausse de tout ce qui précède

Il est donc crucial de:

- Assurer leur fonctionnement
- Réduire la probabilité de survenue et/ou l'ampleur des dommages d'une perturbation, d'une défaillance ou d'une destruction d'infrastructures critiques
- Réduire le plus possible la durée de non-disponibilité.

Contre quels types de risques?

Défaillances organisationnelles

Erreurs humaines

Défaillances techniques

Attaques et menaces délibérées

Risques induits par les systèmes d'information

Etat des lieux

1- Identification des organismes à infrastructures d'information critiques

2- Suivi personnalisé dans :

- La préparation des besoins (cahier des charges acquisition, audit, etc)
- Le développement de compétences (Formations, séminaire, etc)
- La gestion des événements /incidents (veille, détection, alerte, traitement)
- Le suivi du plan d'action
- Le suivi des indicateurs de sécurité

- Un seul pool (Pour les infrastructures d'information, Pour les prestataires)

- Gouvernance de la sécurité

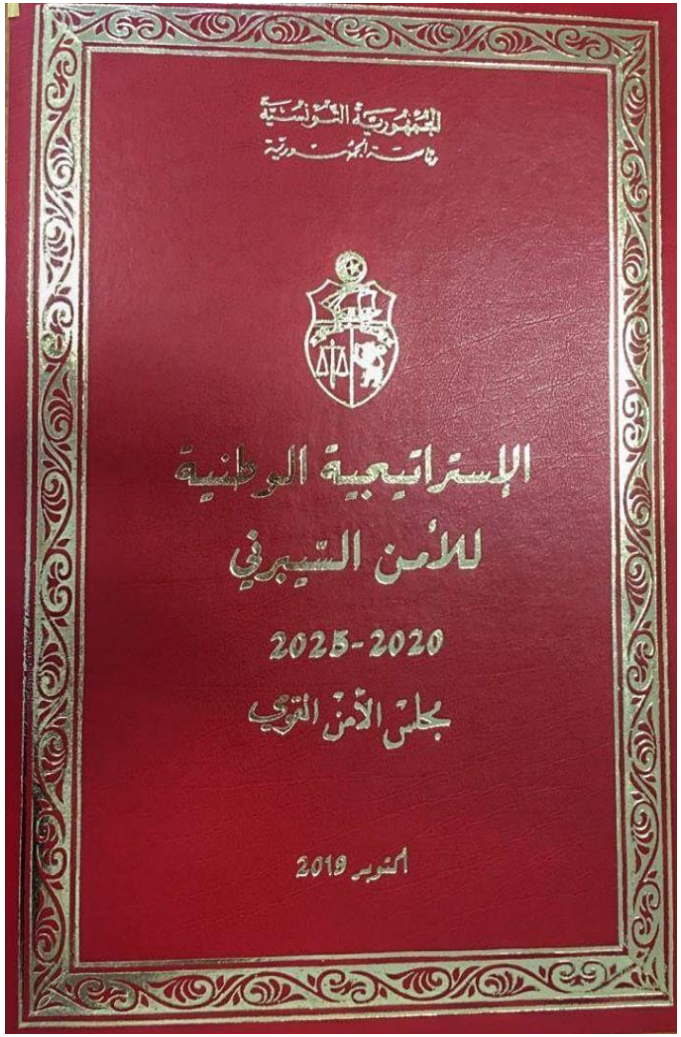
- Instruments juridiques insuffisants (audit périodique + déclaration d'incident)

- Niveau de maturité disparate

- Perception insuffisamment claire sur les infrastructures critiques

- Périmètre : IT VS Système de production

Etat des lieux



La tunisie dispose désormais d'une

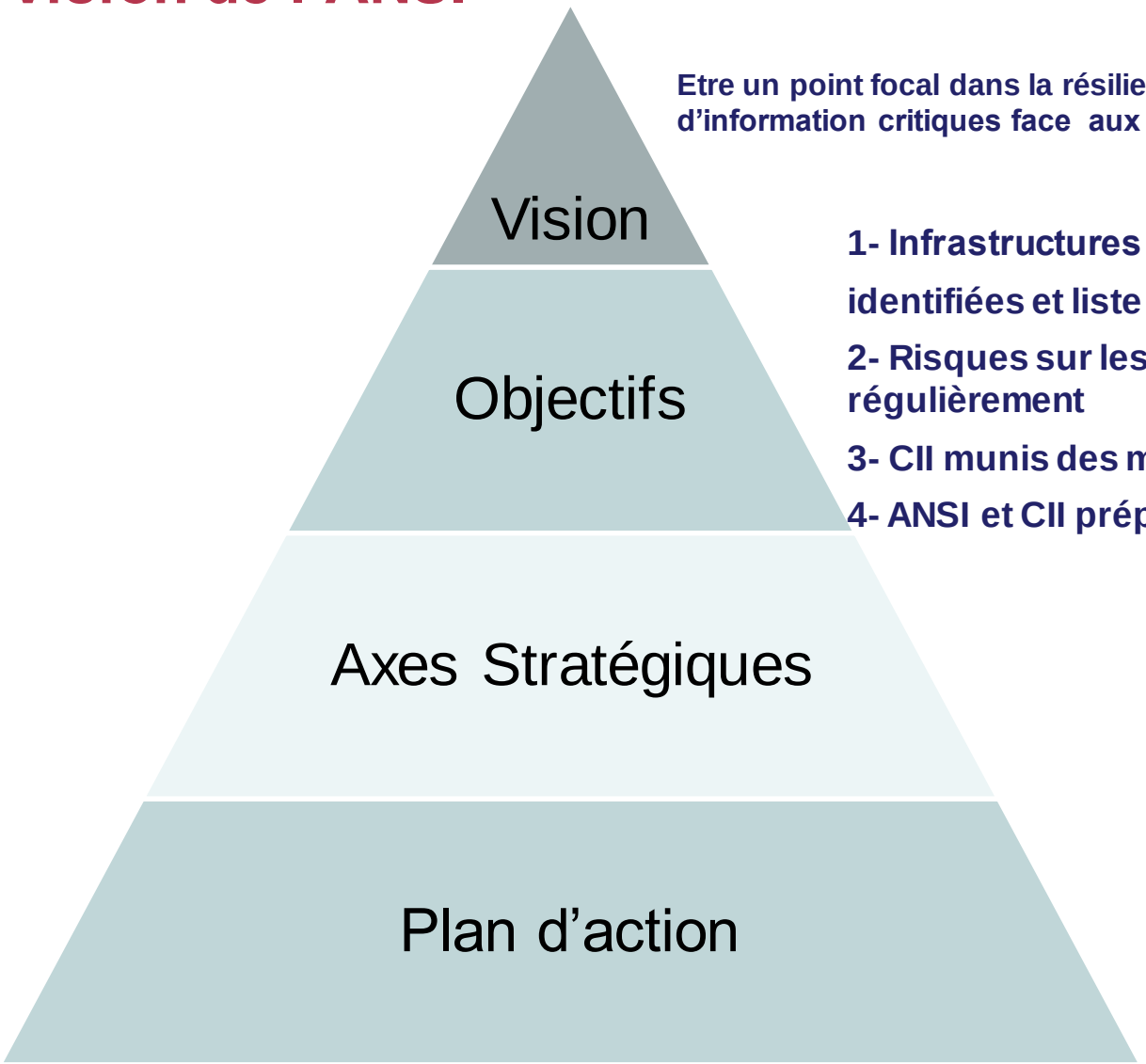
stratégie de cybersécurité

Approuvée par le conseil de la sécurité nationale

Vision de l'ANSI

Etre un point focal dans la résilience des infrastructures d'information critiques face aux risques cybernétiques

Vision de l'ANSI



Etre un point focal dans la résilience des infrastructures d'information critiques face aux risques cybernétiques

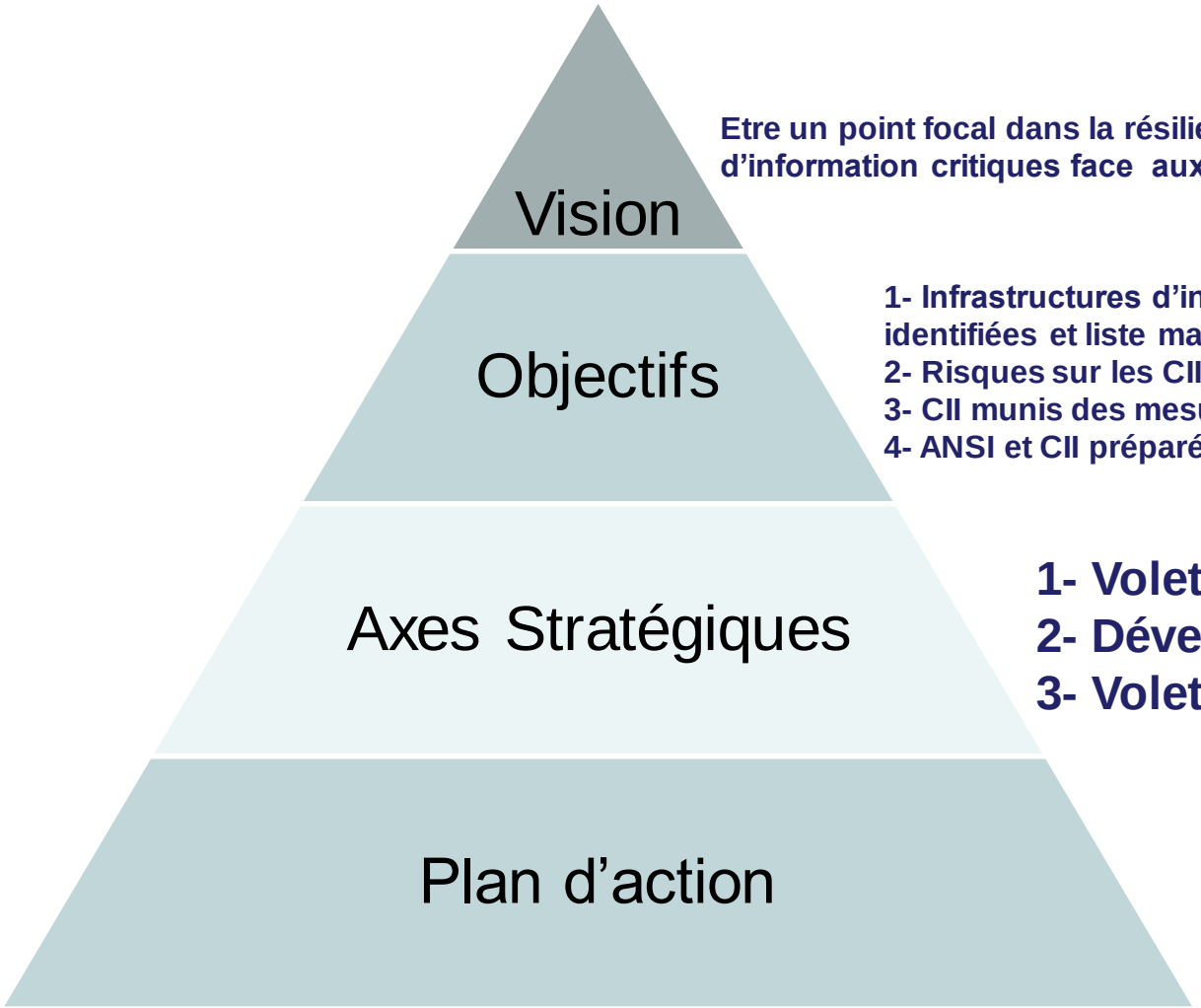
1- Infrastructures d'information critiques identifiées et liste maintenue

2- Risques sur les CIIs identifiés et évalués régulièrement

3- CII munis des mesures préventives nécessaires

4- ANSI et CII préparés pour les situations de crise

Vision de l'ANSI



Etre un point focal dans la résilience des infrastructures d'information critiques face aux risques cybernétiques

1- Infrastructures d'information critiques identifiées et liste maintenue
2- Risques sur les CIIs identifiés et évalués régulièrement
3- CII munis des mesures préventives nécessaires
4- ANSI et CII préparés pour les situations de crise

1- Volet organisationnel
2- Développement de capacités
3- Volet opérationnel

Vision de l'ANSI

Etre un point focal pour coordonner la résilience des infrastructures d'information critiques face aux risques cybernétiques

1- Infrastructures d'information critiques identifiées et liste maintenue
2- Risques sur les CIIs identifiés et évalués régulièrement
3- CII munis des mesures préventives nécessaires
4- ANSI et CII préparés pour les situations de crise

1- Volet organisationnel
2- Développement des capacités
3- Volet opérationnel

1- Assise juridique (Gouvernance, Rôles et responsabilités, suivi et gestion de crise)
2- Renforcement des capacités
3- Framework d'échange d'information

Vision de l'ANSI

Plan d'action

Assisse juridique

- Modèle de gouvernance
- Identification des CII
- Obligation des CIIs
- Gestion de crise majeure

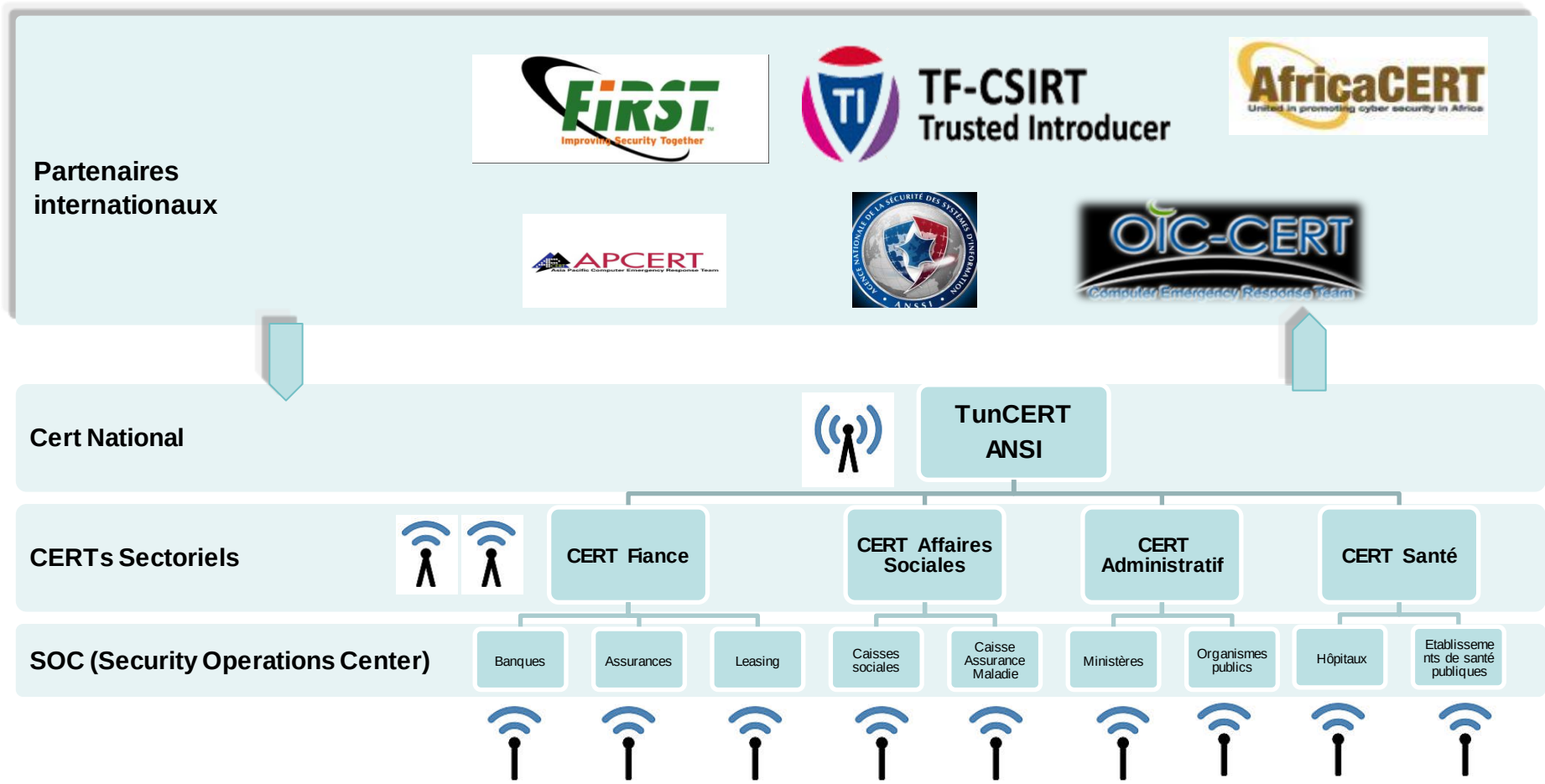
Renforcement des capacités

- Formation ciblées (exp: mastère ANSI-supcom)
- Exercices et siimulations (exp : cyberdrill)
- Prestataires de service spécialisés
- Boite à outils du RSSI (Self assessment service, SAHER Entreprise, modèles de documents)

Framework de partage, d'échange d'information et de coordination

- Informations sur les attaques (exp : ANTIDDOS)
- CERT Sectoriel
- SOC entreprise (SPINGY)

Framework national de sécurité – Schéma projeté



tunCERT
Tunisian Computer Emergency ResponseTeam

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Référentiel d'Audit de la Sécurité des Systèmes d'Information

Évolutions du document

Version	Date	Nature des modifications
1.0	19/12/2018	Version initiale
1.1	05/01/2015	Version mise à jour
1.2	03/06/2015	MAJ des intitulés des domaines
2.0	10/05/2018	Alignement avec la norme ISO/IEC 27002 :2013
2.1	14/10/2019	MAJ suite à la publication de l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique.

Pour toute remarque

Contact	@ Mail	Téléphone
Direction de l'Audit de la Sécurité des Systèmes d'Information	audit@ansi.tn	71 846 020

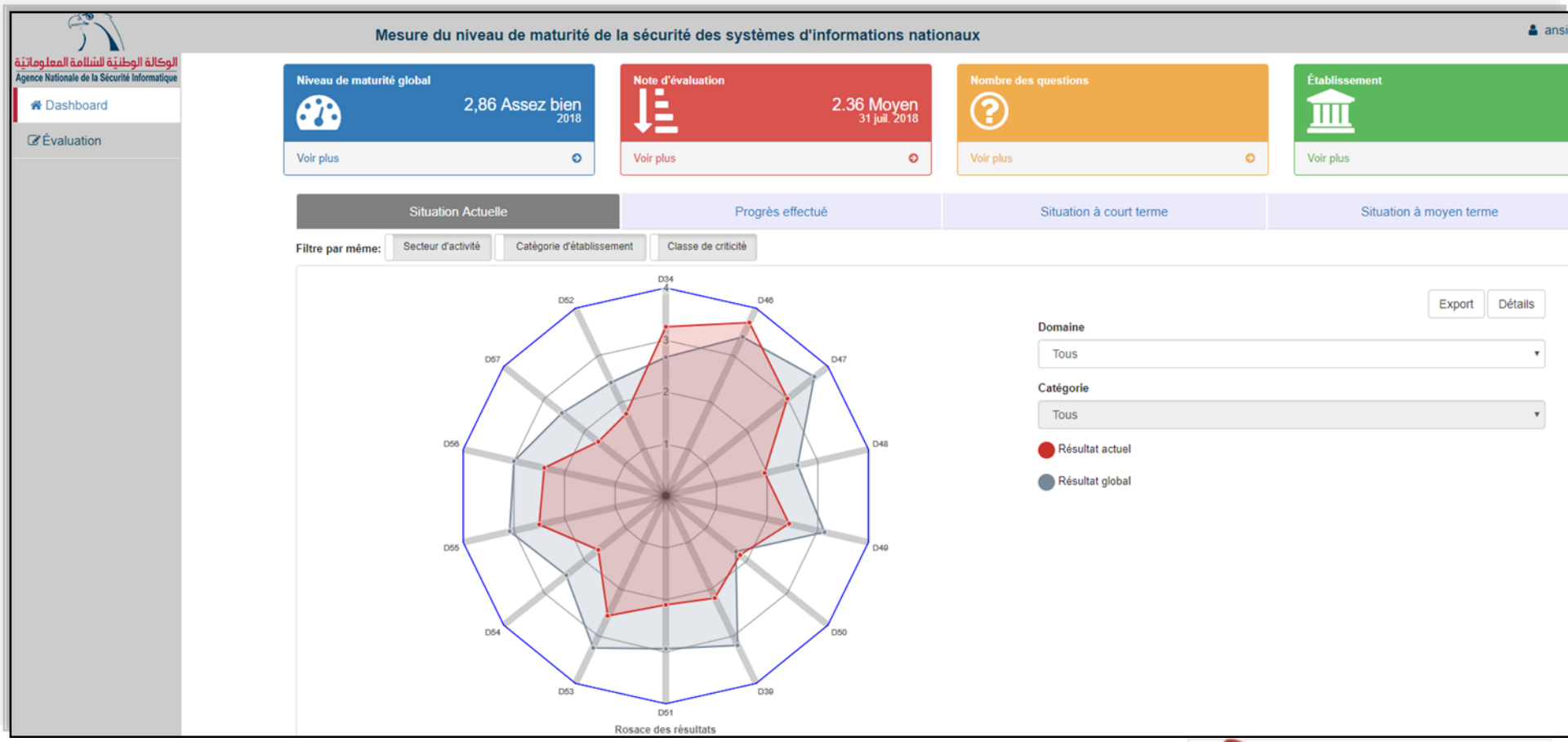
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Modèle de Rapport d'Audit de la Sécurité des Systèmes d'Information

(En application à la loi n°5 de 2004)

Évolutions du document

Version	Date	Nature des modifications
1.0	19/12/2014	Version initiale
1.1	03/06/2015	Ajout de recommandations
1.2	03/05/2017	Mise à jour des domaines de l'audit
1.3	14/10/2019	MAJ suite à la publication de l'arrêté du ministre des technologies de la communication et de l'économie numérique et du ministre du développement, de l'investissement et de la coopération internationale du 01 Octobre 2019, fixant le cahier des charges relatif à l'exercice de l'activité d'audit dans le domaine de la sécurité informatique.


Mesure du niveau de maturité de la sécurité des systèmes d'informations nationaux
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique
Dashboard
Évaluation
Niveau de maturité global
2,86 Assez bien
2018
Voir plus
Note d'évaluation
2.36 Moyen
31 juil. 2018
Voir plus
Nombre des questions
Voir plus
Établissement
Voir plus
Situation Actuelle
Progrès effectué
Situation à court terme
Situation à moyen terme
Filtre par même:
Secteur d'activité
Catégorie d'établissement
Classe de criticité
D34
D46
D47
D48
D49
D50
D39
D51
D53
D54
D55
D56
D57
D52
Export
Détails
Domaine
Tous
Catégorie
Tous
Résultat actuel
Résultat global
Rosace des résultats

Les défis

- **Processus d'élaboration et d'approbation des textes réglementaires**
- **Pénurie des compétences qualifiées**
- **Résistance au changement**
- **Systèmes vieillissants**

Merci pour votre attention

awatef.homri@ansi.tn