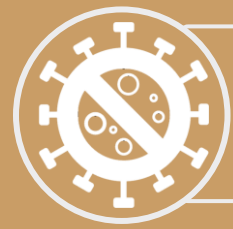
rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Panel :

« Cyber résilience : Menaces et opportunités pour le secteur financier en Tunisie »



FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!

Cadre réglementaire

Loi n°5-2004 du 03 février 2004 relative à la sécurité informatique

- Création de l'ANSI: Agence Nationale de la Sécurité Informatique
- L'audit de la sécurité des SI
- La déclaration des incidents cybernétiques

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Décret n° 2004-1250 du 25 mai 2004, fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et les procédures suivi de l'application des recommandations contenues dans le rapport d'audit.

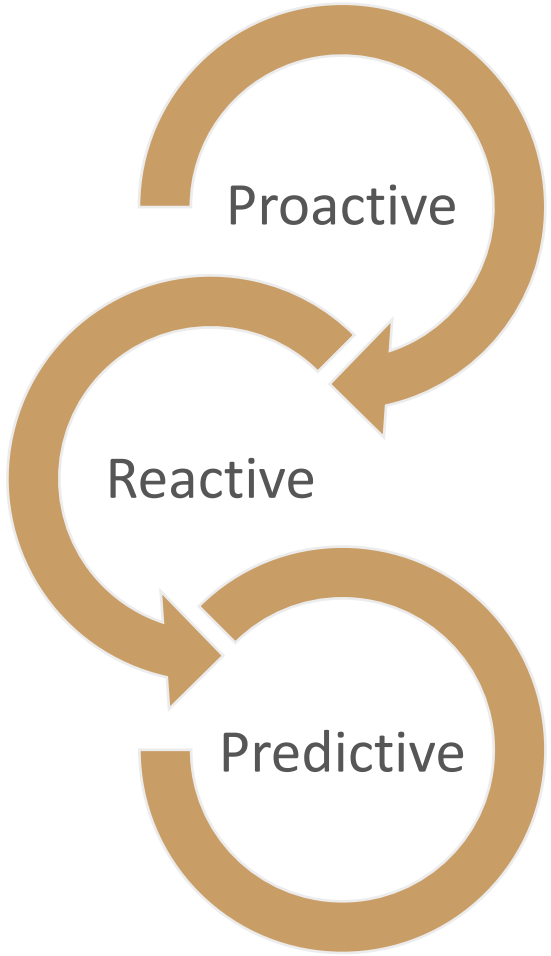
- Art. 2 : Organismes soumis à l'obligation d'audit
- Art. 3 : Phases d'une opération d'audit
- Art. 4 : Rapport d'audit
- Art. 5 : Périodicité de l'audit

arrêté ministériel 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.

- Condition d'accès à la certification PP et PM
- Obligations de l'expert auditeur

Les missions de l'ANSI

L'ANSI effectue un contrôle général des systèmes informatiques et des réseaux relevant des divers organismes publics et privés



- Développement des compétences (Auditeurs, RSSIs, etc)
- Sensibilisation
- Audit de la sécurité des systèmes d'information
- Assistance dans les projets de sécurité SSI
- Conformité (réglementaire, Standards internationaux, etc)
- Guides de bonnes pratiques
- Veille sur le cyberespace national
- Exercices cyberdrill

- Coordination internationale
- Investigation suite aux incidents
- Assistance pour le traitement des incidents

- SAHER: plateforme de Monitoring du cyberespace national
- Plateforme Anti DDOS

Gouvernance de la SSI

Cas des établissements publics en Tunisie

➔ **Circulaire n°24** du 05 novembre **2020** relative au renforcement des mesures de sécurité dans les établissements publiques.

➔ stipule entre autre:

✓ la création d'un comité de pilotage « comité de sécurité »,

✓ La création d'une cellule opérationnelle de sécurité,

✓ la nomination d'un RSSI rattaché à la haute direction.

الجمهورية التونسية
رئاسة الحكومة

تونس في 05 2020

منشور عدد 24

من السيد رئيس الحكومة
إلى
السيدات والسادة الوزراء وكتاب الدولة والولاة ورؤساء المؤسسات والمنشآت العمومية

الموضوع: حول تدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.
المراجع - القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية.
- الاستراتيجية الوطنية للأمن السيبرني.
- المنشور عدد 19 لسنة 2007 المؤرخ في 17 أفريل 2007 المتعلق بتدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.

في إطار تعزيز سلامة النظم والشبكات بالهياكل العمومية وبهدف ضمان ديمومتها وتوفر معطياتها، يتعين اتخاذ التدابير التالية:

بخصوص الإطار التنظيمي:

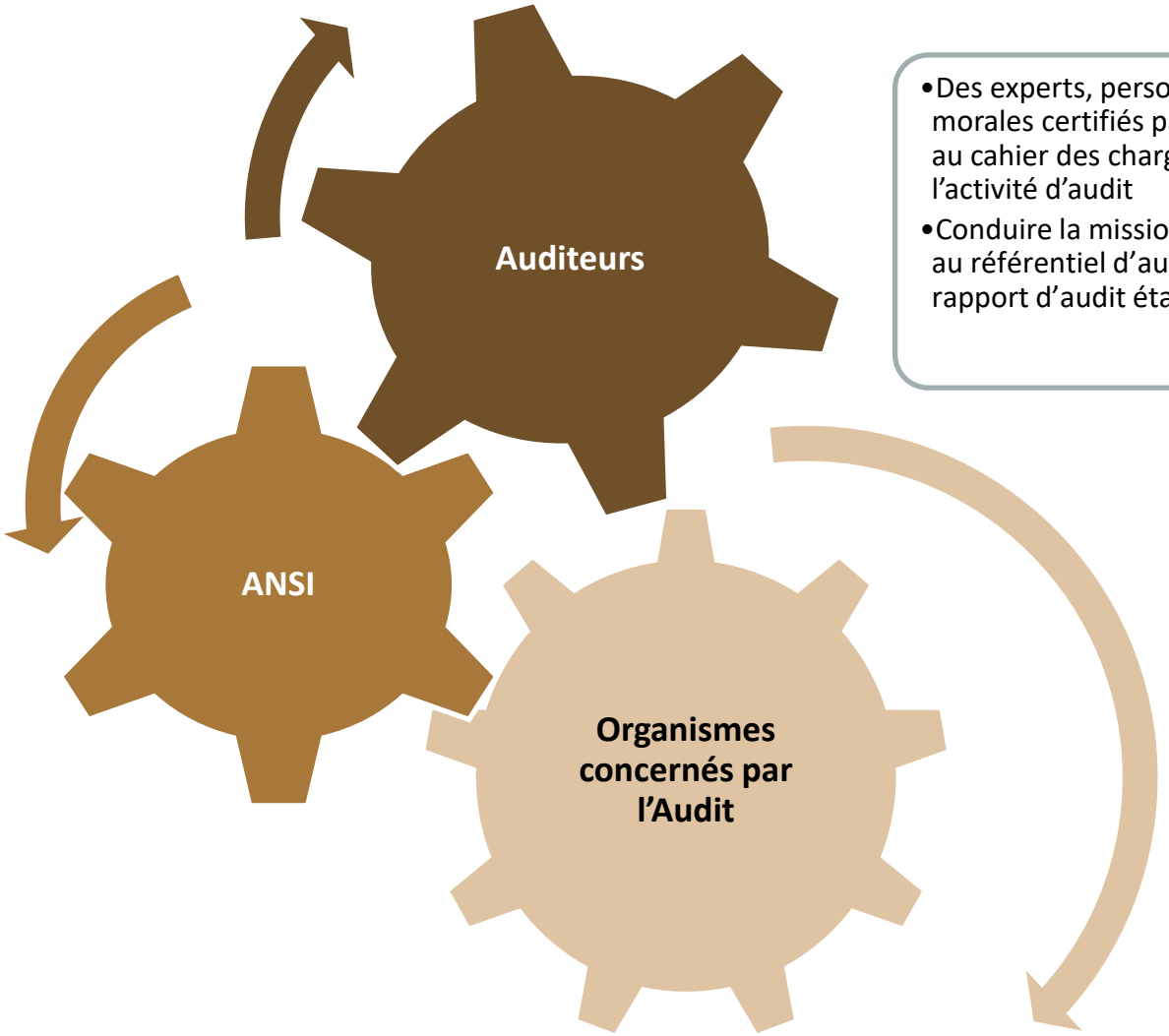
-إحداث "لجنة سلامة النظم المعلوماتية (Comité de Sécurité)" يترأسها المسؤول الأول عن الهيكل أو من ينوبه وتضم خاصة المسؤولين عن استغلال النظم المعلوماتية حسب نشاط الهيكل. وتكلف هذه اللجنة خاصة باعتماد ومتابعة تنفيذ سياسة السلامة المتعلقة بالنشاط الأساسي بالهيكل (Politique de Sécurité) وكذلك بمتابعة تنفيذ المخططات العمليّة المتعلقة باستمرارية النشاط والخدمات والتوصيات المنبثقة عن تقارير التدقيق المنجزة طبقا لأحكام قانون السلامة المعلوماتية.

تجتمع اللجنة بصفة دورية مرة كل ستة أشهر على الأقل وكلما اقتضت الضرورة لدراسة المسائل المرتبطة بالسلامة المعلوماتية.

بخصوص الإشراف العملياتي:

- تعيين إطار مسؤول عن سلامة النظام المعلوماتي (RSS) يكون المخاطب الوحيد لمصالح الوكالة الوطنية للسلامة المعلوماتية على أن يتوفر لديه التكوين المختص والخبرة المناسبة لتنفيذ مهامه استئناسا بالمعايير الدولية المعمول بها وأن يمارس مهامه تحت الاشراف المباشر للمسؤول الأول عن الهيكل.
- إحداث خلية مختصة يترأسها مسؤول عن سلامة النظام المعلوماتي. وتكلف هذه الخليّة خاصة بما يلي :

Les trois acteurs de l'audit réglementaire



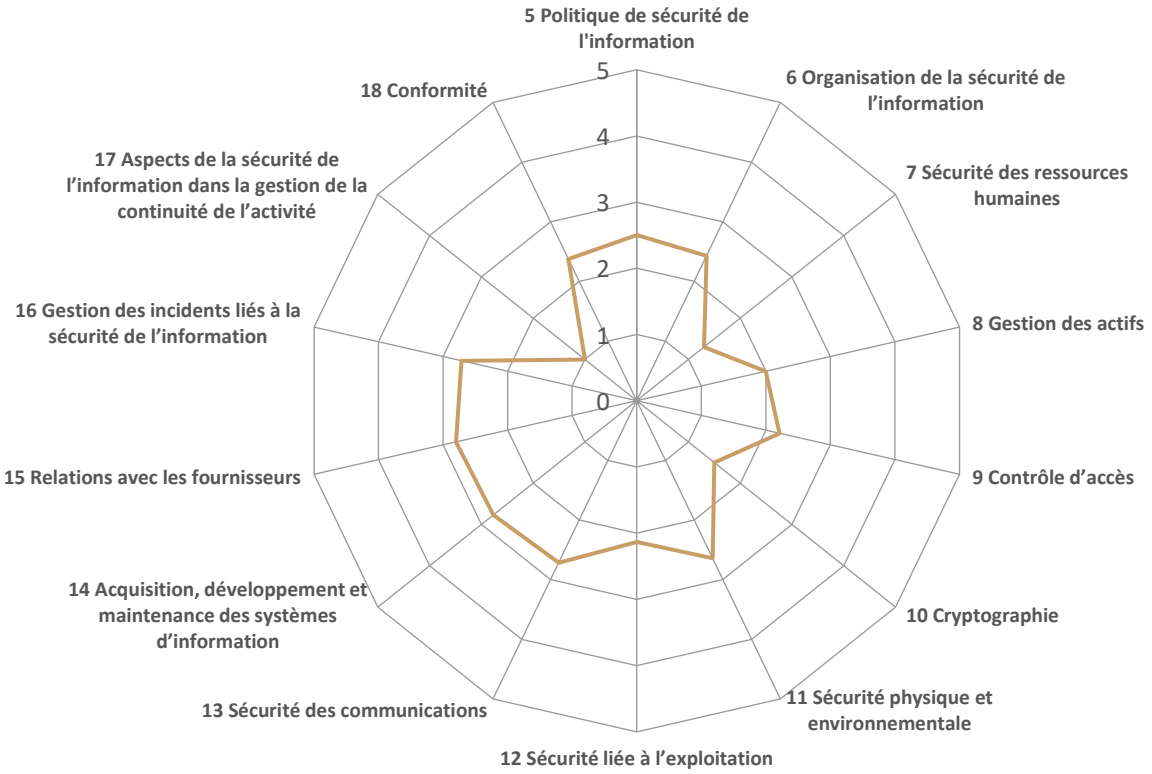
- Des experts, personnes physiques Ou morales certifiés par l'ANSI conformément au cahier des charges relatif à l'exercice de l'activité d'audit
- Conduire la mission d'audit conformément au référentiel d'audit et le modèle du rapport d'audit établis par l'ANSI

- Certification et suivi des experts auditeurs
- Assistance des organismes concernés par l'audit
- Evaluation des missions d'audit
- Développement des documents requis pour l'audit (Référentiel d'audit, Modèle de rapport d'audit, Modèle de termes de références, …)
- Statistiques et indicateurs résultant de l'audit réglementaire

- Toutes entreprises publiques
- Les opérateurs de réseaux publics de télécommunication et les fournisseurs des services de télécommunications et internet.
- Les entreprises dont les réseaux informatiques sont interconnectés à travers des réseaux externes de télécommunication.
- Les entreprises qui procèdent au traitement automatisé des données personnelles de leurs clients dans le cadre de fourniture de leurs services à travers les réseaux de télécommunications.

Audit réglementaire et cyber résilience

- Le référentiel de l'audit réglementaire utilise comme norme de référence: ISO 27002 .
- Il permet une évaluation de l'efficacité et du niveau de maturité des différentes mesures de sécurité de la norme ISO 27002 selon les 5 niveaux du modèle de maturité de capacité (SSE-CMM).
- L'application de l'audit réglementaire et de ses recommandations prépare et encourage l'organisme à l'adoption d'une démarche de mise en place d'un SMSI (Système de Management de la Sécurité de l'Information) conforme à la norme ISO 27001.



Audit réglementaire et cyber résilience

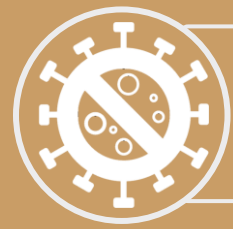
Les mesures de sécurité de la norme ISO 27002:2022 dont la valeur de l'attribut « Domaines de sécurité » est: #résilience

Id de la mesure dans ISO 27002	Nome de la mesure	Description de la mesure
5.1	**Politiques de sécurité de l'information**	Il convient de définir une politique de sécurité de l'information et des politiques portant sur des thèmes, de les faire approuver par la direction, de les publier, de les communiquer et d'en demander confirmation au personnel et aux parties intéressées concernés, ainsi que de les réviser à intervalles planifiés et si des changements notoires interviennent.
5.2	**Fonctions et responsabilités liées à la sécurité de l'information**	Il convient de définir et d'attribuer les fonctions et responsabilités liées à la sécurité de l'information selon les besoins de l'organisation.
5.5	**Relations avec les autorités**	Il convient que l'organisation établisse et entretienne des relations avec les autorités compétentes.
5.7	**Intelligence des menaces**	Il convient de recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces.
5.29	**Sécurité de l'information durant une perturbation**	Il convient que l'organisation planifie la procédure de maintien de la sécurité de l'information au niveau approprié en cas de perturbation.
5.30	**Préparation des TIC pour la continuité d'activité**	Il convient de planifier, de mettre en œuvre, de gérer et de tester la préparation des TIC en fonction des objectifs de continuité d'activité et des exigences de continuité des TIC.
7.13	**Maintenance du matériel**	Il convient d'entretenir le matériel correctement.
8.14	**Redondance des moyens de traitement de l'information**	Il convient de mettre en œuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité.

rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Merci pour votre attention



FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!