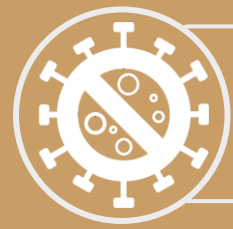
rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Panel :

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

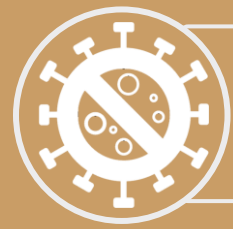


FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!

rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

« Présentation de réglementations à l'échelle internationale »



FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!

DORA (Digital Operational Resilience Act)

le nouvel enjeu de la résilience bancaire

- La place centrale et stratégique des systèmes d'information dans les systèmes bancaires (digitalisation des processus, robotisation, IA…) expose l'ensemble des institutions financières à un risque informatique ou numérique croissant pouvant affaiblir leur résilience opérationnelle, dans un contexte marqué par la multiplication de cyberattaques de plus en plus sophistiquées
- Le recours aux prestataires externes qui opèrent pour un certain nombre d'organisations, et deviennent malgré eux des vecteurs de contamination en cas d'incident participe à cette augmentation du niveau d'exposition du secteur bancaire au risque cyber
- Ces dernières années, les pannes de système et les cybermenaces généralisées, ainsi que les effets de la pandémie de Covid-19 ont placé la résilience opérationnelle en tête de liste des priorités des régulateurs financiers

DORA (Digital Operational Resilience Act)

le nouvel enjeu de la résilience bancaire

- C'est dans ce contexte que la Commission européenne a adopté le 24 septembre 2020, le « digital financial package » visant à garantir que le secteur financier puisse tirer parti des possibilités offertes par les technologies de l'information et de la communication (TIC).

- Le projet de règlement européen « DORA » (Digital Operational Resilience Act), qui en est issu, a vocation à renforcer la cybersécurité de l'ensemble du secteur financier

- Ce règlement s'appliquera aux acteurs du secteur financier d'ici la fin 2022 et plus particulièrement aux Organismes d'Importances Vitales (OIV) dans le secteur de la finance

Qu'est-ce que le projet DORA ?

DORA s'articule autour de cinq piliers représentés ci-dessous

Projet de règlement DORA

PILIERS	OBJECTIFS	IMPACT OPÉRATIONNEL
Risques TIC	Limiter les perturbations causées par des incidents via un dispositif de gestion et de surveillance adapté.	• Mise en place d'un organe de gestion responsable. • Mise en place d'un cadre de gestion des risques et des activités associées (identification, protection et prévention, détection, réaction et rétablissement, apprentissage et évolution, communication de crise).
Rapport d'incident	Développer le dispositif de gestion des incidents TIC pour pouvoir réagir aux cyberattaques	• Classification standardisée des incidents • Déclaration obligatoire et normalisée des incidents majeurs.
Tests de résilience	Tester l'efficacité du cadre de gestion des risques TIC	• Déployer un programme complet d'essais (tests techniques et d'intrusion). • Mener des tests à grande échelle par des testeurs indépendants tous les 3 ans
Risques Tiers	Gestion des prestataires tiers (prestataires de fonctions critiques et essentielles)	• Mise en oeuvre d'une stratégie et d'une politique en la matière et tenue d'un registre d'information standardisé. • Respect des lignes directrices pour l'évaluation précontractuelle et le contenu du contrat.
Partage d'information	Définir une stratégie de communication pour favoriser l'échange sur les cybermenaces	• Appliquer les lignes directrices sur les modalités de partage des informations.

Organiser la gouvernance pour la gestion des risques informatiques autour d'un organe de direction dédié

- La place centrale et stratégique des systèmes d'information dans les systèmes bancaires (digitalisation des processus, robotisation, IA…) expose l'ensemble des institutions financières à un risque informatique ou numérique croissant pouvant affaiblir leur résilience opérationnelle, dans un contexte marqué par la multiplication de cyberattaques de plus en plus sophistiquées
- Le recours aux prestataires externes qui opèrent pour un certain nombre d'organisations, et deviennent malgré eux des vecteurs de contamination en cas d'incident participe à cette augmentation du niveau d'exposition du secteur bancaire au risque cyber
- Ces dernières années, les pannes de système et les cybermenaces généralisées, ainsi que les effets de la pandémie de Covid-19 ont placé la résilience opérationnelle en tête de liste des priorités des régulateurs financiers

Organiser la gouvernance pour la gestion des risques informatiques autour d'un organe de direction dédié

Un organe de direction sera pleinement responsable de la gestion des risques informatiques de l'entité financière concernée.

Le projet de règlement DORA décline la responsabilité de l'organe de direction en un certain nombre d'exigences :

- Définir clairement **les rôles et les responsabilités** pour toutes les fonctions liées à l'informatique ;
- **Réaliser des examens périodiques** de la gestion des risques informatiques ainsi que des processus d'approbation et de contrôle ;
- **Allouer un budget approprié à la résilience opérationnelle numérique** ainsi que pour les formations concernant ces risques informatiques.

Plus précisément chaque organisme financier devra mettre en place :

- une **cartographie des risques**,
- des mécanismes de détection des **activités anormales** (seuils d'alerte, critère de déclenchement des processus de détection des incidents),
- des politiques de **sauvegardes**, des méthodes de récupération et des politiques de continuité des activités informatiques,
- des **procédures de réponse** aux incidents et de rétablissement pour garantir la continuité des activités informatiques ainsi qu'une stratégie de communication en cas d'incidents,
- des **formations** au profit de l'ensemble du personnel concerné

Création d'un processus harmonisé et centralisé de notification des incidents informatiques

Le projet de règlement DORA met en place un **dispositif de signalement harmonisé** des incidents auprès d'un guichet unique et selon une **méthodologie standard de classification** des incidents par des critères spécifiques, tels que :

- le nombre d'utilisateurs ou de contrepartie financières touchés,
- la durée de l'incident,
- la répartition géographique des zones touchées,
- la perte de données occasionnée,
- la gravité des effets de l'incident et la criticité des services touchés,
- l'impact économique de l'incident.

Selon cette méthodologie, les incidents désignés comme majeurs devront être signalés à l'autorité de régulation, au plus tard à la fin du jour ouvrable de leur survenance, selon un modèle précis. Un rapport de suivi devra également être fourni à l'autorité de régulation dans la semaine puis dans le mois suivant la notification de l'incident

Obligation de réaliser des tests de résilience opérationnelle numérique

- Le projet de règlement DORA impose de réaliser un programme complet de tests de résilience numérique, selon la taille, l'activité et le profil de risque de l'entité financière concernée.
- **Les organisations les plus critiques** (l'Autorité bancaire européenne, l'Autorité européenne des marchés financiers et l'Autorité européenne des assurances et des pensions professionnelles) devront réaliser tous les trois ans des **tests de pénétration** fondés sur la menace par des testeurs indépendants qui répondent à un certain nombre d'exigences, notamment concernant leur expertise technique.

Neutralisation des risques liés aux tiers prestataires de services informatiques

Les organismes financiers devront disposer d'un **niveau de contrôle et de surveillance de leurs tiers prestataires de services informatiques suffisant** (en particulier ceux désignés comme critiques) et mettre en place une surveillance spécifique des fournisseurs qui sont **essentiels** pour le marché dans son ensemble.

Plus précisément, avant de conclure avec un tiers prestataire, chaque organisme financier, devra :

- Identifier si celui-ci couvre une **fonction critique** et évaluer tous les risques pertinents ;
- Vérifier les qualités requises du tiers prestataire tout au long du **processus de sélection et d'évaluation**;
- S'assurer qu'il respecte des normes élevées, adéquates et actualisées en matière de **sécurité de l'information**;
- Formaliser un **registre des fournisseurs** et des prestations rendues.

Chaque accord contractuel devra respecter les exigences posées par l'article 27 du projet de règlement et notamment les **motifs de résiliation** qui doivent être liés à un risque ou à une preuve de non-conformité du fournisseur et s'accompagner de périodes de transitions obligatoires.

Enfin, les fournisseurs essentiels devront être évalués chaque année au regard des exigences de résilience et notamment : la disponibilité, la continuité, l'intégrité des données, la sécurité physique, les processus de gestion des risques, la gouvernance, la portabilité, les tests etc..

Le partage d'informations entre les entités financières

- La proposition de règlement DORA définit une stratégie de communication afin de promouvoir l'échange d'informations sur les cybermenaces entre entités financières et introduit des lignes directrices pour mettre en place des accords de partage d'informations, en incluant des exigences de confidentialité et l'obligation d'informer l'autorité de régulation.
- Cette proposition de règlement est encore en discussion entre le Conseil et le Parlement européen mais devrait entrer en vigueur courant 2022.
- Il est donc impératif pour l'ensemble des organismes financiers de **lancer dès à présent ces chantiers de mise en conformité**.

Qu'est ce que la DSP2

2ème Directive sur les Services de paiement

- La norme de sécurisation des paiements, la DSP2, s'applique depuis le 15 mai à l'ensemble des achats en ligne dès 30 euros. Elle permet de lutter contre les fraudes par carte bancaire qui sont, avec le développement du e-commerce, de plus en plus fréquentes. Ce système d'«authentification forte» assure la protection des commerçants et rassure les clients. DSP2 a un impact significatif sur l'écosystème du paiement. Elle impacte les banques, les nouveaux acteurs FinTech du paiement, mais également les consommateurs
- La directive sur les services de paiement (DSP2) a pour objectif de favoriser l'innovation, la concurrence et l'efficience. Elle instaure notamment des normes de sécurité plus strictes pour les paiements en ligne afin de renforcer la confiance des consommateurs dans les achats en ligne.
- Les mesures de sécurité énoncées dans les normes techniques de réglementation découlent de deux objectifs clés de la DSP2 :
  - Assurer la protection des consommateurs
  - Renforcer la concurrence et garantir des conditions de concurrence équitables dans un marché en mutation rapide.

DSP2, authentification forte : des exigences de sécurité plus strictes

- La protection des consommateurs est assurée par une amélioration de la sécurité des paiements électroniques. C'est la raison pour laquelle les normes techniques de réglementation instaurent des exigences de sécurité que les prestataires de services de paiement doivent respecter lorsqu'ils traitent des opérations de paiement ou fournissent des services connexes. Les prestataires de services de paiement incluent les banques et les autres établissements de paiement. Ces normes définissent les exigences à remplir pour permettre une « authentification forte » des clients.
- Avant DSP2, l'authentification forte restait seulement recommandée. Avec DSP2, elle devient obligatoire.
- Les normes techniques prévues dans la DSP2 font de l'authentification forte la condition de base pour que le client puisse accéder à son compte de paiement ou effectuer des paiements en ligne. Cela implique que, pour prouver son identité, l'utilisateur devra répondre au moins à deux des trois conditions suivantes :
  - Un mot de passe ou un code que seul l'utilisateur connaît
  - Un appareil (téléphone mobile, carte à puce, etc) que seul l'utilisateur possède
  - Une caractéristique personnelle du client (empreinte digitale, reconnaissance vocale, ou faciale).

Directive politique présidentielle 21 (PPD-21)

- La Presidential Policy Directive 21 (PPD-21) est une directive sur la protection et la résilience des infrastructures aux États-Unis qui vise à renforcer et à sécuriser les infrastructures critiques du pays. L'ancien président Barack Obama a publié le PPD-21 en 2013 pour favoriser une plus grande intégration et coopération entre les organisations publiques et privées. L'objectif de la directive est de réduire les vulnérabilités, d'identifier et de perturber les menaces, de minimiser les conséquences et d'accélérer les efforts d'intervention et de rétablissement liés aux infrastructures critiques
- **Résilience :** La directive définit *la résilience* comme la capacité de se préparer et de s'adapter aux conditions changeantes et aux perturbations. La résilience comprend la capacité de résister et de se remettre d'attaques délibérées, d'accidents ou de menaces ou d'incidents naturels. La directive appelait également le gouvernement fédéral à s'engager avec des partenaires internationaux pour renforcer la sécurité et la résilience des infrastructures critiques nationales, ainsi que des infrastructures critiques à l'extérieur des États-Unis dont dépend la nation

Directive politique présidentielle 21 (PPD-21)

- La Presidential Policy Directive 21 (PPD-21) est une directive sur la protection et la résilience des infrastructures aux États-Unis qui vise à renforcer et à sécuriser les infrastructures critiques du pays. L'ancien président Barack Obama a publié le PPD-21 en 2013 pour favoriser une plus grande intégration et coopération entre les organisations publiques et privées. L'objectif de la directive est de réduire les vulnérabilités, d'identifier et de perturber les menaces, de minimiser les conséquences et d'accélérer les efforts d'intervention et de rétablissement liés aux infrastructures critiques
- **Résilience :** La directive définit *la résilience* comme la capacité de se préparer et de s'adapter aux conditions changeantes et aux perturbations. La résilience comprend la capacité de résister et de se remettre d'attaques délibérées, d'accidents ou de menaces ou d'incidents naturels. La directive appelait également le gouvernement fédéral à s'engager avec des partenaires internationaux pour renforcer la sécurité et la résilience des infrastructures critiques nationales, ainsi que des infrastructures critiques à l'extérieur des États-Unis dont dépend la nation

Sécurité ou Résilience ? De quoi parlons-nous

Cette directive, qui peut être vue comme une référence en la matière définit les termes suivants :

- **La sécurité** consiste à réduire le risque pour les infrastructures par des moyens physiques ou mesures de cyberdéfense à des intrusions, les attaques ou les effets des catastrophes naturelles ou causées par l'homme.
  - ***Exemples de mesures de sécurité:***
  - *Badge aux portes d'entrée*
  - *Utiliser un logiciel antivirus*
  - *Clôture autour des bâtiments*
  - *Verrouillage des écrans d'ordinateur*

- **La résilience** est la capacité à préparer et à s'adapter à des conditions changeantes, de résister et de récupérer rapidement suite à des perturbations subies. La résilience comprend la capacité de résister et de se remettre d'attaques délibérées, d'accidents, ou de catastrophes naturelles ou encore d'incidents.

  - ***Exemples de mesures de résilience:***
  - *Élaboration d'un plan de continuité d'activité*
  - *Prévoir un générateur électrique de secours*
  - *Utilisation de matériaux de construction durables*

Sécurité ou Résilience ? De quoi parlons-nous

Le préfixe **Cyber**, pour sa part fait référence à toutes les techniques liées à la société du numérique et notamment à l'informatique et à l'internet.

On pourrait donc résumer de la façon suivante :

- *la **cybersécurité** consiste à réduire les risques d'intrusion, d'attaques ou les effets de catastrophes naturelles ou causées par l'homme dans le cadre de l'utilisation des moyens informatiques et de communication,*

- alors que

- *la **cyber-résilience** est la capacité à se préparer et s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication.*

Sécurité ou Résilience ? De quoi parlons-nous

Des différences essentielles

- Il résulte de ces deux définitions que le périmètre de cybersécurité couvre essentiellement la réduction des risques et la résolution des incidents de sécurité de l'information alors que la cyber-résilience est beaucoup plus large et couvre à la fois la préparation à subir des attaques (prévention) et par dessus tout à pouvoir continuer et reprendre une activité business normale (correction) très rapidement suite à une attaque, une catastrophe naturelle ou des incidents liés à la sécurité de l'information.

La sécurité n'est-elle donc pas suffisante en soi?

- **La réponse est clairement négative**. La sécurité vise à prévenir les incidents de sécurité et à gérer ces incidents mais ne prépare pas l'Organisation à faire face aux conséquences d'une cyber-attaque et à récupérer ses aptitudes à créer de la valeur après en avoir été la victime.

Sécurité ou Résilience ? De quoi parlons-nous

Pouvons-nous utiliser les mêmes référentiels et normes ?

- Là encore **la réponse est négative**, du moins en partie. La cybersécurité pouvant être vue comme un sous ensemble de la cyber-résilience, il est clair que les référentiels et normes en matière de sécurité constitueront une première étape mais il convient d'élargir très sensiblement le périmètre pour couvrir les aspects de cyber-résilience.

Quelques exemples des normes et de référentiels :

Sécurité :

- ISO 27001 – Systèmes de Management de la sécurité de l'information – Exigences
- ISO 27002 – Code de bonne pratique pour le management de la sécurité de l'information
- **Cyber-résilience :**
- RESILIA – Bonnes pratiques de Cyber-Résilience
- ISO 22301 – Systèmes de management de la continuité d'activité – Exigences

Sécurité ou Résilience ? De quoi parlons-nous

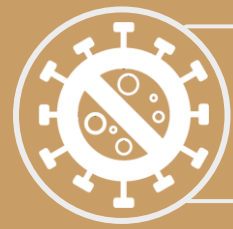
- La **cyber-résilience** vise à gérer la sécurité en adoptant une approche globale impliquant à la fois les individus, les processus et la technologie. Elle impose une méthodologie à la fois solide et évolutive de gestion, d'analyse et d'optimisation des risques. Elle se pose comme le meilleur garant du capital informationnel des entreprises, organisations, états et individus. La cyber-résilience s'appuie sur cinq piliers que sont la préparation/ l'identification, la protection, la détection, la résolution des problèmes et la récupération. Dans cette approche, il est donc essentiel de se poser les bonnes questions, d'adopter les bonnes mesures et de les réévaluer à un rythme régulier et de façon pragmatique, afin de gérer au mieux les cyber-risques.

- Dès lors que les entreprises ont compris que les cyber-attaques les affecteront tôt ou tard, indépendamment des efforts de prévention qu'elles auront mis en oeuvre et seront couronnées de succès, elles peuvent passer à l'étape suivante: la conception et l'implémentation d'un Programme de Cyber-Résilience (PCR). Un PCR englobe bien sûr les concepts de défense et de prévention, mais va au-delà de ces mesures pour mettre l'accent sur la réponse et la résilience de l'organisation dans les moments de crise.

rsbp Programme régional PME Tunisie

Banque Européenne pour la Reconstruction et le Développement

Merci de votre attention



FORMEZ VOUS EN LIGNE EN TOUTE SECURITE!