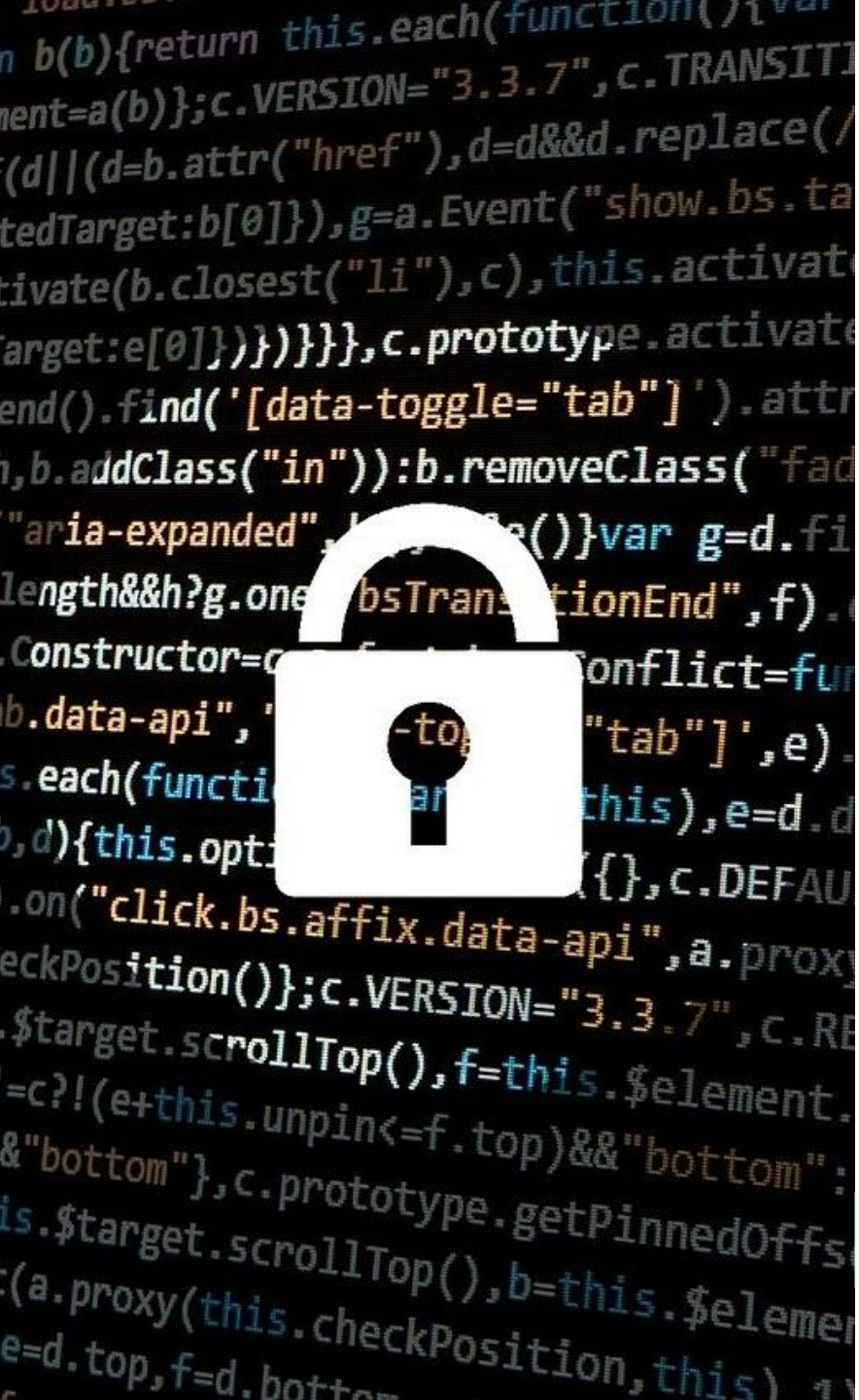


Ailancy
make it happen!

DORA - Digital Operational Resilience Act

Vers un niveau élevé de résilience opérationnelle numérique

Nos convictions & savoir-faire

27 avril 2023

SOMMAIRE

DORA ou comment atteindre un niveau élevé de résilience opérationnelle numérique

Motivations

- Le **numérique** et les **Technologies de l'Information et de la Communication** (TIC) sont une source d'**opportunités** mais présentent aussi des **risques** liés à **l'interdépendance au-delà des frontières des réseaux et infrastructures critiques** dans un contexte d'accroissement des **incidents** et des **cyberattaques**.
- Les **risques informatiques** menacent la **résilience opérationnelle**, les performances et la stabilité du système financier de l'UE. De plus, ils ne font pas toujours l'objet d'une attention poussée dans la couverture des risques opérationnels.
- Ce règlement s'inscrit dans le cadre de travaux plus vastes, au niveaux européen et international, pour renforcer la **cybersécurité** des services financiers.

➡ **Permettre à l'Europe de tirer parti de tous les avantages du numérique, au sein d'un cadre garant de la résilience opérationnelle numérique au niveau de l'ensemble du secteur financier**

Cadre d'application

- **Risque cyber** plutôt que tous les risques informatiques
- **Un périmètre très large :**
  - Entités financières : les établissements de crédit, de paiement, les entreprises d'investissement, de monnaie électronique, infrastructures de marché, les organismes d'assurance
  - Autres acteurs clés du secteur financier : Agences de notation
  - Les prestataires tiers de services TIC pour le secteur financier

Base juridique

- Observation de nombreuses **disparités, sur le plan législatif** et en terme de surveillance, avec un cadre réglementaire jusqu'alors fragmenté et hétérogène de la gestion des risques informatiques au niveau de l'UE.
- Cela crée un obstacle au **marché unique** des services financiers dans l'Union Européenne. DORA souhaite donc **harmoniser** ces différentes mesures avec un cadre unique et prend en compte les orientations et exigences existantes.
- Le règlement DORA s'appuie sur la directive NIS et la directive DORA **met en cohérence les directives** existantes (MIFID, Solvabilité, IORP, DSP, AIFM, OPCVM…)

➡ **Simplification et convergence des textes au niveau européen pour permettre une meilleure supervision des risques.**

Subsidiarité & Proportionnalité

- **Subsidiarité –** Dépendance du secteur financier européen à l'égard de tiers prestataires de services informatiques.
- **Proportionnalité –** Prise en compte des caractéristiques propres des entités financières en terme de taille, de secteur d'activité et d'exposition au risque.

DORA permet l'homogénéisation de la réglementation au niveau européen

La multiplication des menaces liées au TIC met en péril la stabilité du système financier européen. De plus, les exigences relatives à la prise en compte de ces menaces n'était pas harmonisée au niveau européen.

- Application directe pour les 27 pays de l'UE
- Textes de niveau 2 RTS/ITS
- Supervision des autorités européennes de surveillance

Harmonise au niveau européen les dispositifs de gestion du risque TIC

DORA

Modifie d'autres directives pour assurer une cohérence au niveau européen

- DSP II
- MIFID II
- Solvabilité II
- CRD
- BRDD
- IORP II
- OPCVM/ AIFM
- Audit

DORA : de la gestion du risque opérationnel informatique à la résilience opérationnelle numérique en 4 piliers

1. Gouvernance et gestion des risques liés aux TIC

- Gouvernance appropriée : la direction de l'entité est responsable de la gestion des risques TIC
- Cadre de gestion des risques adapté sur les 3 LoDs : identification des risques, protection par le suivi et le contrôle permanent, détection des anomalies, réponse et rétablissement via des politiques et plans de continuité, mise en œuvre de politiques de sauvegardes et de restaurations, apprentissage et évolution au travers de tests, d'examens post-incident et d'un dispositif de formation

2. Gestion, classification et notification des incidents liés aux TIC

- Mise en place d'indicateurs d'alerte et de processus de gestion des incidents liés aux TIC incluant une analyse des causes et la mise en œuvre de plans de remédiation et/ou d'atténuation
- Classification des incidents et des cybermenaces
- Information des parties prenantes et notification des autorités de contrôle lors d'un incident majeur
- Partage d'informations et de renseignements en rapport avec les cybermenaces et vulnérabilités

3. Tests de résilience opérationnelle numérique

- Programmes de tests de résilience opérationnelle numérique fondé sur les risques
- Les tests sont entrepris par des parties indépendantes, soit externes, soit internes
- Recueil des résultats de tests, classification des vulnérabilités et mise en œuvre des mesures correctives nécessaires
- Différents types de tests en fonction de la taille et de l'activité de l'entité

4. Gestion des risques liés aux prestataires tiers de services TIC

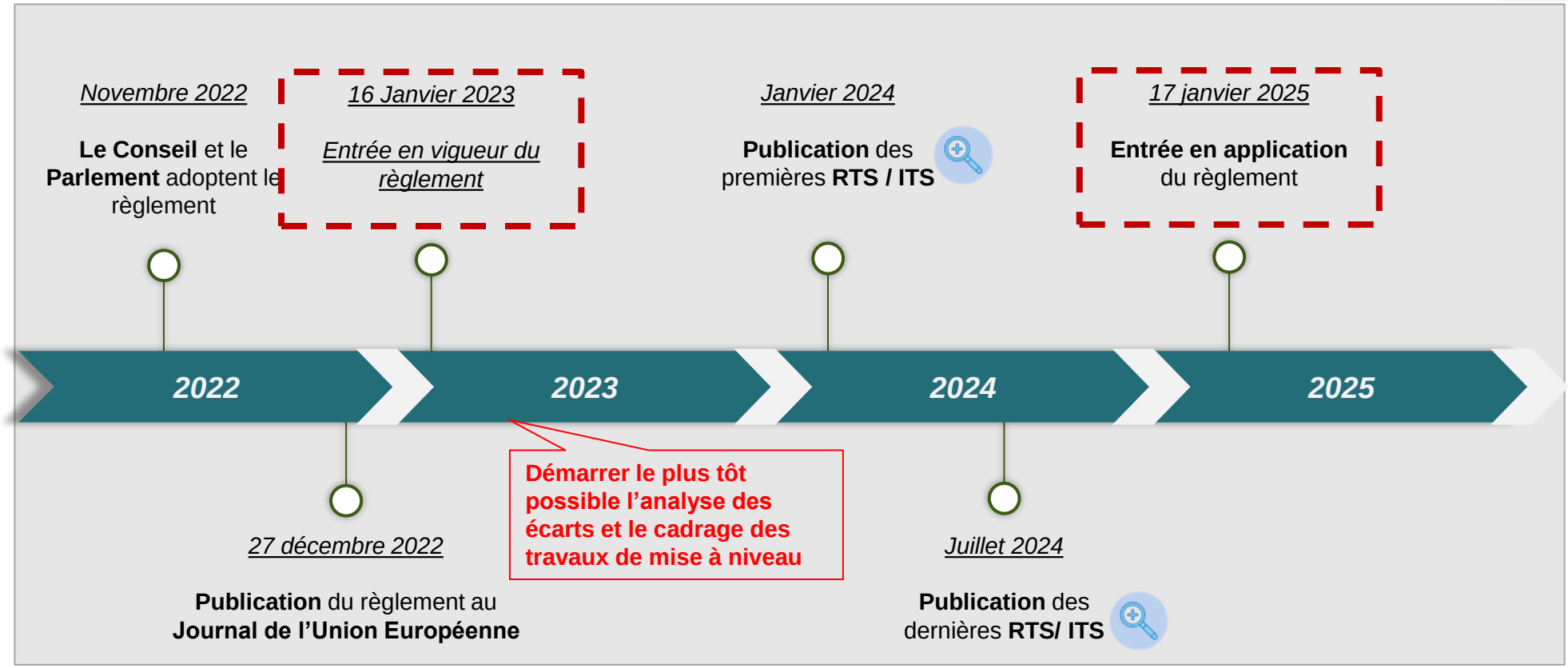
- Mise en place d'une stratégie pour appréhender les risques liés aux tiers fournisseurs de TIC en tant que partie intégrante du risque lié au TIC et suivant le principes de proportionnalité
- Tenue d'un registre et information des autorités sur les nouveaux accords passés avec certains tiers
- Revue des contrats passés avec les tiers et évaluation du risque de concentration
- Implication des tiers dans les tests

Les chantiers majeurs de DORA

1. Adapter la gouvernance et assurer la formation des acteurs clefs
2. Evaluer ou réévaluer la stratégie de gestion du risque TIC et mettre à jour le cadre normatif
3. Adapter, les processus et procédures de l'entité
4. Faire l'inventaire des TIC et réévaluer leurs risques
5. Prévoir des plans de communication
6. Mettre en place des tests à l'échelle de l'organisation
7. Améliorer le contrôle des tiers

Un calendrier sur 2 ans entre entrée en vigueur et mise en application

Initiée par les **Orientations de l'EBA de 2019,** la **mise en place d'un cadre réglementaire européen** permettant une **résilience forte** en cas d'incidents graves liés aux TIC au sein de l'Union Européenne se poursuit. Le règlement est **entré en vigueur le 16 janvier 2023** et sa mise en œuvre sera de 24 mois au fur et à mesure de la publication des RTS



Inutile de courir, il faut partir à temps…
… en se basant sur l'existant pour évaluer les écarts et planifier la mise à niveau

Les RTS et ITS donneront un éclairage plus concret sur la mise en œuvre

Les Autorités Européenne de Surveillance vont élaborer des Regulatory et Implementing Technical Standards qui ont pour but de spécifier la mise en œuvre de certains éléments évoqués dans le règlement (normes, formats, outils, modèles). Les RTS/ ITS doivent être publiés par les superviseurs 12 à 18 mois après la date d'entrée en vigueur du règlement.

	1 Cadre de gestion des risques	2 Classification des menaces	3 Notifications d'incidents	4 Tests	5 Tiers	6 Contenu des accords contractuels
Date soumission à la CE*	**17/01/2024**	**17/01/2024**	**17/07/2024**	**17/07/2024**	**17/01/2024**	**17/07/2024**
Contenu des RTS/ITS	- *Politiques, procédures, protocoles et outils de sécurité des TIC* - *Contrôle des droits d'accès* - *Détection des activités anormales* - *PCA, PRA et tests associés* - *Réexamination du cadre de gestion des risques*	- *Critères d'importance significative pour déterminer si un incident est majeur*	- *Procédure d'alerte des autorités en cas d'incident majeur, sous quel délai* - *Définir les formulaires les modèles et procédures pour notifier un incident **(ITS)***	- *Critères pour classifier les établissement de crédit importants* - *Normes sur l'utilisation de testeurs internes* - *Portée et méthodologie pour chaque phase de test.* - *Etapes de remédiation*	- *Modèle standard du registre d'information sur les accords contractuels passés avec les tiers **(ITS)*** - *Contenu de la politique relative à l'externalisation de TIC critiques*	- *Les éléments pour fournir une description détaillée des services que l'entité sous-traite*

*CE = Commission Européenne

SOMMAIRE

Nos convictions

Contactez nos équipes pour découvrir les convictions d'Ailancy sur le règlement DORA.

Conviction 1 – Inutile de courir, il faut partir à temps… en se basant sur l'existant pour évaluer les écarts

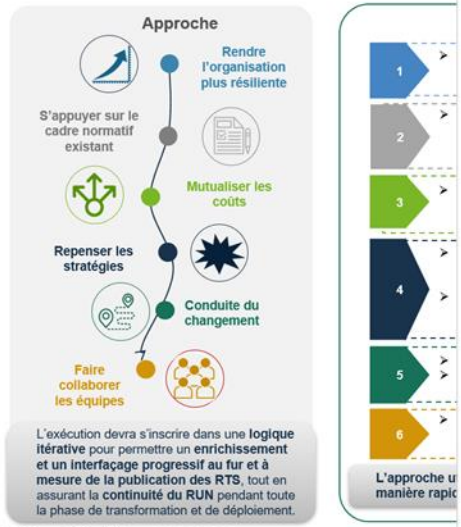
- DORA constitue un renforcement du cadre réglementaire existant et a vocation à remplacer la directive NIS pour le secteur financier. Des orientations ont été poussées depuis 2018 par les AES tant pour les banques (EBA, ESMA) et pour les compagnies d'assurance (EIOPA).
- Les entités financières installées en France doivent donc déjà avoir un cadre de gestion de leurs risques informatiques, qui lui-même s'intègre dans le cadre de gouvernance et de contrôle interne. Notamm
  du risque informatique (7 Juillet 2021) pour les entrepris
  soumises au contrôle de l'ACPR.

Piliers DORA	L'existant attendu
Pilier 1 Gouvernance et gestion des risques liés aux TIC	✓ Responsabilité des dirigeants e surveillance ✓ Dispositif de gestion du risque i ✓ Politique de sécurité du système sécurité physique et logique des ✓ Sensibilisation et formation des ✓ Surveillance et contrôle des sys ✓ Cadre de conduite clair et effica informatiques ✓ Politique globale de continuité d ✓ Dispositif de gestion de la conti
Piliers 2, 3 et 4	✓ Pilier 2: Processus de détection ✓ Pilier 3: Tests de poursuite des ✓ Pilier 4: Gestion des tiers et ten d'externalisation

AILANCY | CONFIDENTIEL

Conviction 2 – Les facteurs clefs pour une mise en œuvre réussie de DORA

La mise en œuvre de DORA demande une réflexion stratégique d'appréhension des risques TIC et une adaptation opérationnelle de la gouvernance et des processus internes de gestion des risques.



L'exécution devra s'inscrire dans une **logique itérative** pour permettre un **enrichissement et un interfaçage progressif au fur et à mesure de la publication des RTS**, tout en assurant la **continuité du RUN** pendant toute la phase de transformation et de déploiement.

L'approche u
manière rapid

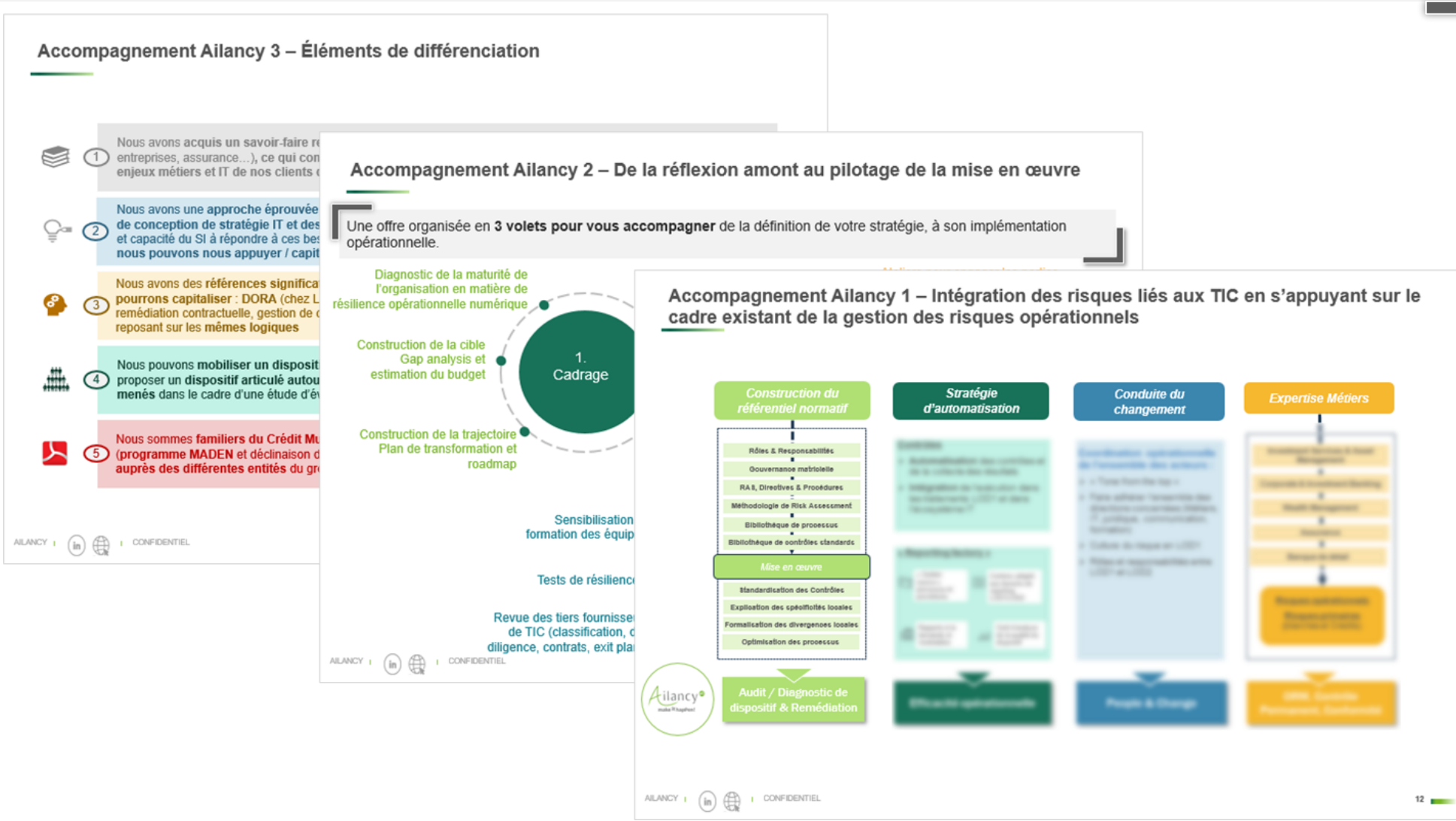
AILANCY | CONFIDENTIEL

Conviction 3 – Les facteurs clefs de succès de la démarche

AILANCY | CONFIDENTIEL 13

Accompagnement Ailancy

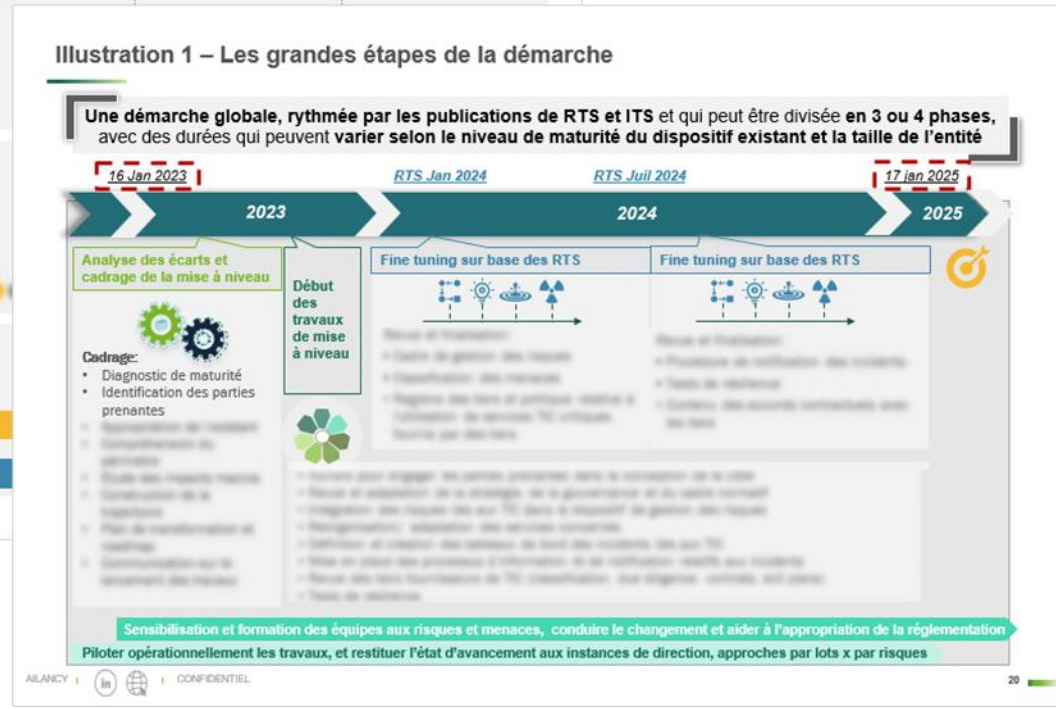
Contactez nos équipes pour découvrir l'accompagnement proposé par Ailancy sur le règlement DORA.



SOMMAIRE

Approche détaillée

Contactez nos équipes pour découvrir notre approche détaillée du règlement DORA.



Mise en œuvre

Contactez nos équipes pour découvrir la mise en œuvre du règlement DORA selon Ailancy.

Pilier 1

Mise en œuvre 1 – Les étapes pour fiabiliser le cadre de gestion des risques liés aux TIC

Les établissements financiers disposent déjà d'un cadre de gouvernance et de contrôle interne destiné à garantir une gestion efficace et prudente des risques et sur lequel ils peuvent s'appuyer pour y intégrer les aspect liés aux TIC.

	Quoi	Comment	Qui
1	Gouvernance		
2	Cadre normative : mise à jour des politiques, procédures, protocoles et outils		
3	Cartographie des risques, évaluation du risque inhérent, revue périodique (min 1 fois par an)		
4	Prevention des risques		
5	Analyse et reporting des résultats de contrôles et des incidents		

AILANCY | CONFIDENTIEL

Pilier 2

Mise en œuvre 2 – Rationalisation des notifications d'incidents liés à l'informatique

La gestion opérationnelle des inc
délai raisonnable et de mettre en

Rapports aux autorités surveilla

Lorsqu'un incident majeur survient, l
fournit aux auto
- *Une notification*
- *Un rapport interme*
- *Un rappo*

Juillet 24

Plan de communicat

Lorsqu'un incident survient et affe
clients de l'entité, celle-ci doit les in
dans les plus brefs

AILANCY | CONFIDENTIEL

Pilier 3

Mise en œuvre 3 – Application de tests de résilience opérationnelle numérique

Les tests de résilience opératio
entité financière, d'y remédier e

1
2
3
4

AILANCY | CONFIDENTIEL

Pilier 4

Mise en œuvre 4 – Tiers prestataires de services informatiques

L'entité financière doit revoir son approche stratégique vis-à-vis de ses tiers du point de vue de la criticité des services TIC délégués mais aussi d'un point de vue contractuel. Elle doit par ailleurs impliquer les tiers dans les procédures de contrôle et de tests.

Janvier 24

Janvier 24
Juillet 24

Janvier 24

AILANCY | CONFIDENTIEL

Donnera lieux à des RTS

18

SOMMAIRE

Ailancy accompagne ses clients dans l'implémentation et l'optimisation des dispositifs de gestion des risques sur les 3 lignes de défense

Contactez nos équipes pour connaitre nos références

Challenger les existants (organisation, pratiques managériales, processus…), y compris en matière de répartition des rôles & responsabilités et de gouvernance

S'appuyer sur des **benchmarks / best practices** afin d'identifier des leviers d'optimisation / simplification ayant fait la preuve de leur efficacité

Designing an organizational culture is allowed by working on individual behaviors and on collective practices (for example governance, project management, processes).

S'appuyer sur des **consultants experts** dans leur domaine d'activité pour challenger l'existant et proposer une roadmap robuste pour **tenir les délais**

Une maitrise des processus et outils de la fonction Risques et des méthodologies d'audit / diagnostic

Le cabinet dont le métier est d'accompagner ses clients vers l'excellence opérationnelle

Une approche sur mesure visant des résultats tangibles et mesurables

Un déroulé rythmé de mission accompagné d'un pilotage resserré

Ailancy vous accompagne sur tout le cycle de vie de la transformation

Élaborer la stratégie de développement

> Étude de marché et positionnement stratégique
> Stratégies opérationnelles
> Cadrage et accompagnement de projets de développement

Améliorer la compétitivité de l'organisation

> Refonte de processus et des organisations
> Accompagnement de restructurations et fusions
> Recherche de partenariats, d'outsourcing et de synergies

S'adapter aux contraintes réglementaires

> Expertise forte notamment sur : ESG, MIF II, DDA, RGPD, DSP2, PRIIPS, …
> Conduite de veille, analyse d'impacts et appui à la mise en œuvre
> Optimisation du risk management et du dispositif de conformité

Conduire de grands projets de transformation

> Dispositifs PMO & pilotage de programme
> Conduite de projets en méthodologie Agile
> Mobilisation d'équipes pluridisciplinaires

Faire évoluer le Système d'information

> Construction de schéma directeur informatique
> Aide au choix de progiciels
> Appui à la spécifications métier

Réussir sa transition digitale

> Définition de plan de transformation digitale et aide à la déclinaison
> Expertise en matière d'Open Banking, APIs, blockchain
> Appui sur la présence au sein de l'écosystème Fintechs

Une offre de service complète dédiée à l'industrie financière

Banque de détail & SFS
Services d'investissement & Asset Management
Banque de Financement et d'Investissement
Assurance
Gestion patrimoniale & Assurance Vie
Finance, Risque, Conformité
Innovation & Digital
Leadership & Change

Conseil en organisation et management

- Stratégie de développement
- Compétitivité des organisations
- Risques & conformité
- Conduite de grands projets
- Transformation des SI
- Accélération digitale
- Coaching, Formation, Mobilisation

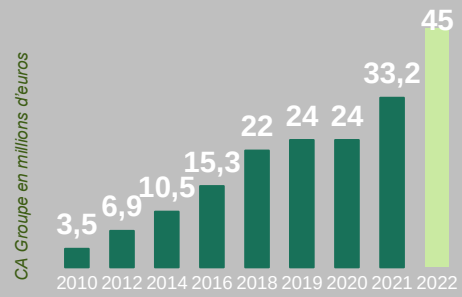
Expertises & Solutions

- Exécution et pilotage de projets IT
- Expertises techniques / fonctionnelles
- Digital, UX & Data
- Cloud & Security
- Development Factory

+270 consultants répartis sur 5 entités

+1000 missions réalisées

Une croissance continue depuis 15 ans



2 marques | 5 entités | 4 sites

Ailancy – make it happen!

PARIS	CASABLANCA	LUXEMBOURG
+180 consultants	+10 consultants	+5 consultants

avanty – Expertise & Solutions by Ailancy

PARIS	TUNIS
+70 collaborateurs	+5 collaborateurs

Consultants SI salariés
(PO, PM, BA, SM, UX, DEV, Architectes…)

+300 Experts indépendants

SOMMAIRE

Les éléments clés du contexte et de la réglementation

- *Contexte du règlement*
- *Agenda*
- *Les piliers*

Nos convictions, notre offre d'accompagnement et nos éléments de différenciation

Notre approche détaillée

Notre savoir-faire

Annexes

- *Zoom sur les piliers DORA*

Détail de chaque pilier

Contactez nos équipes pour découvrir le détail de chaque pilier du règlement DORA.

Franck Grenier, Associé

Franck.grenier@ailancy.com
Mob. : +33 6 60 93 66 57

Guillaume Louvet, Associé

guillaume.louvet@ailancy.com
Tel : +33 6 89 50 51 24

Javotte Rullaud, Directeur

javotte.rullaud@ailancy.com
Mob. : +33 6 17 72 61 94

Ailancy
make it happen!

32 rue de Ponthieu
75008 Paris

+33 (0)1.80.18.11.60

www.ailancy.com

Suivez-nous sur les réseaux

Ailancy
AilancyConseil
Ailancy