France Invest

Règlement DORA : Comment accélérer votre mise en conformité d'ici janvier 2025?

24 septembre 2024

Vos intervenants

Romain Camus
Associé gestion des risques technologiques
PwC France et Maghreb

romain.camus@pwc.com
+33 (0) 6 75 75 51 94

Monique Tavares
Directrice – Experte réglementaire

monique.tavares@pwc.com
+33 (0)6 87 70 58 95

Agenda

#1	Vue d’ensemble du règlement DORA
#2	Vision benchmark de l’état d’avancement du marché
#3	Les sujets clés à appréhender et retour d’expérience
#3.1	La gouvernance
#3.2	Le principe de proportionnalité et périmètre
#3.4	La gestion des incidents TIC
#3.5	La gestion des risques liés aux prestataires de services TIC
#3.6	Les tests de résilience opérationnelle numérique

1

Vue d’ensemble du règlement DORA

Vers une nouvelle approche de la gestion des risques opérationnels

Accélération de la transformation numérique du secteur financier

- Dépendances croissantes à des prestataires de services et à des technologies émergentes
- Montée des incidents et des cyberattaques
- Interdépendances des réseaux, infrastructures critiques interconnectées cross-territoires
- Besoins croissants d'accès à des données internes/externes

Un cadre réglementaire fragmenté et hétérogène en matière de gestion des risques informatiques au niveau de l'UE

La nécessité de renforcer la **résilience opérationnelle numérique** au niveau de l'ensemble du secteur financier

DORA – Les 5 piliers

Le règlement DORA, entré en vigueur le 16 janvier 2023, sera applicable à partir du **17 janvier 2025** dans tous les États membres de l'UE.

DORA : 5 piliers à appréhender pour encadrer la résilience opérationnelle numérique

1. Dispositif de gestion des risques liés aux TIC
2. Gestion, classification et notification des incidents TIC et des cybermenaces
3. Conduite des tests de résilience opérationnelle numérique
4. Gestion des risques liés aux prestataires de service TIC
5. Partage d'informations en matière de cybersécurité

DORA - Périmètre d'application

Entités financières

- Établissements de crédit
- Établissements de paiement
- Établissements de monnaie électronique
- Entreprises d'investissement
- **Sociétés de gestion et gestionnaires de FIA**
- Prestataires de services d'information sur les comptes (PSIC)
- Prestataires de services sur cryptoactifs agréés conformément à MiCA, émetteurs de jetons

- Entreprises d'assurance et de réassurance
- Intermédiaires de (ré)assurance, intermédiaires d'assurance à titre accessoire
- Institutions de retraite professionnelle

- Contreparties centrales
- Référentiels centraux
- Plates-formes de négociation
- Réferentiels centraux
- Prestataires de service de communication de données
- Agences de notation de crédit, Administrateurs d'indices de référence critiques
- Prestataires de services de *crowdfunding*

Prestataires de services TIC

Les entreprises qui fournissent des services numériques et des données notamment les fournisseurs de services informatiques en nuage, de progiciels, de services d'analyse de données, de centres de données, à l'exclusion des fournisseurs de composants matériels et des entreprises qui fournissent des services de communication.

Cadre de gestion des risques liés aux prestataires de services TIC

Sont considérés comme des tiers prestataires de services liés aux TIC

- **les entreprises qui font partie d'un groupe financier** et qui fournissent des services de TIC principalement à leur entreprise mère, ou à des filiales ou des succursales de leur entreprise mère
- **les entités financières qui fournissent des services de TIC à d'autres entités financières**
- **les participants à l'écosystème des services de paiement**

Cadre de supervision UE

Prestataires de services TIC désignés comme « critiques »

à l'exception des

- **entités financières qui fournissent des services de TIC à d'autres entités financières**
- **prestataires de services TIC soumis** à des cadres de supervision établis en vue de soutenir les missions du système européen de banques centrales

DORA – Définitions (1/3)

Qu’est-ce que la résilience opérationnelle numérique ?

> *La capacité d'une entité financière à **développer, garantir et réexaminer son intégrité et sa fiabilité opérationnelles** en assurant, directement ou indirectement, par le recours aux services fournis par des prestataires de services liés aux TIC, l’intégralité des capacités en matière de TIC nécessaires pour garantir la **sécurité des réseaux et des systèmes d’information** qu’elle utilise, et qui sous-tendent **la fourniture continue des services financiers et leur qualité,** y compris **en cas de perturbation.***
>
> *Règlement DORA - article 3 point 1)*

DORA – Définitions (2/3)

Qu'est-ce qu'un service de Technologie de l'information et de la communication (TIC) ?

> *Les services numériques et de données fournis de manière permanente par l'intermédiaire des systèmes de TIC à un ou plusieurs utilisateurs internes ou externes, dont le matériel en tant que service et les services matériels qui englobent la fourniture d'assistance technique au moyen de mises à jour de logiciels ou de micrologiciels réalisées par le fournisseur de matériel, à l'exclusion des services de téléphonie analogique traditionnels*
>
> DORA Règlement Article 3 – point 21

DORA – Définitions (3/3)

Annex III

Type of ICT services

When referring to a type of ICT services in the templates of the register of information, only the identifier (from S01 to S19) of the relevant type of ICT services shall be reported.

Identifier	Type of ICT services	Description
S01	1. ICT project management	Provision of services related to Project Management Officer (PMO).
S02	2. ICT Development	Provision of services related to: business analysis, software design and development, testing.
S03	3. ICT help desk and first level support	Provision of services related to: helpdesk support and first level support on ICT incident
S04	4. ICT security management services	Provision of services related to: ICT security (protection, detection, response and recovering), including security incident handling and forensics.
S05	5. Provision of data	Subscription to the services of data providers. (digital data service)
S06	6. Data analysis	Provision of services related to the support for data analysis. (digital data service)
S07	7. ICT, facilities and hosting services (excluding Cloud services)	Provision of ICT infrastructure, facilities and hosting services. This includes the provision of utilities (energy, heat management…), telecom access and physical security. (excluding Cloud services)
S08	8. Computation	Provision of digital processing capabilities (including data computation). This excludes the computation services performed in the context of a cloud environment.
S09	9. Non-Cloud Data storage	Provision of data storage platform (excluding Cloud services).
S10	10. Telecom carrier	Operations for telecommunication systems and flow management. Traditional analogue telephone services are explicitly excluded as per Article 3(21) of Regulation (EU) 2022/2554
S11	11. Network infrastructure	Provision of network infrastructure
S12	12. Hardware and physical devices	Provision of workstations, phones, servers, data storage devices, appliances, etc. in a form of a service
S13	13. Software licencing (excluding SaaS)	Provision of software run on premises.
S14	14. ICT operation management (including maintenance)	Provision of services related to: infrastructure (systems and hardware except network) configuration, maintenance, installing, capacity management, business continuity management, etc. Including Managed Service Providers (MSP)
S15	15. ICT Consulting	Provision of intellectual / ICT expertise services.
S16	16. ICT Risk management	Verification of compliance with ICT risk management requirements in accordance with Article 6(10) of Regulation (EU) 2022/2554
S17	17. Cloud services: IaaS	Infrastructure-as-a-Service
S18	18. Cloud services: PaaS	Platform-as-a-Service
S19	19. Cloud services: SaaS	Software-as-a-Service

La construction d'un cadre harmonisé et sur plusieurs niveaux

1

Prise en compte des **orientations existantes des AES (EBA, EIOPA, ESMA) et des bonnes pratiques européennes et internationales** destinées à renforcer la cyber-résilience et la résilience opérationnelle du secteur financier

2

Prise en compte des **exigences relatives aux risques liés aux TIC réparties entre différentes directives** de manière implicite ou explicite

DORA

3

Mise en place d'un **cadre unique et commun en matière de résilience opérationnelle numérique** pour le secteur financier

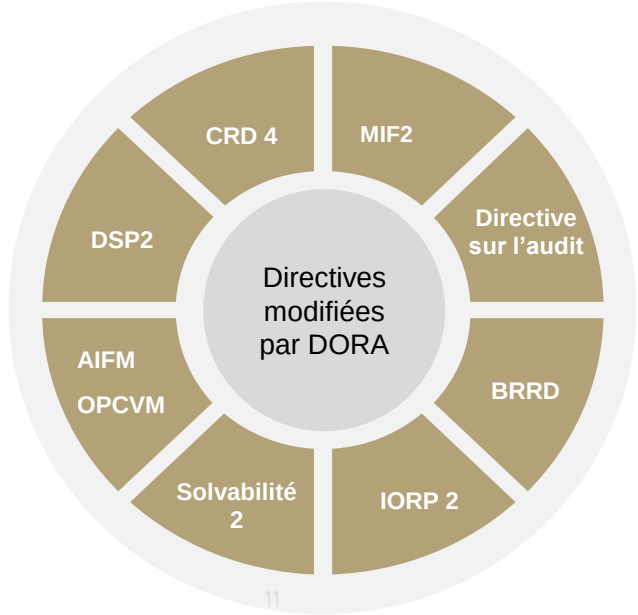
4

Mise en cohérence des directives existantes

Règlement - DORA

- Règlement
- Actes délégués / RTS - ITS
- Orientations

Directive associée DORA



DORA – Où en est-on de la publication des RTS/ITS ?

F Version finale du projet de RTS/ITS — A Adoption par la Commission — P Publication au JOUE

	CADRE DE GESTION DES RISQUES LIÉS AUX TIC	GESTION ET NOTIFICATION DES INCIDENTS TIC ET DES CYBERMENACES	TESTS DE RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE	GESTION DES RISQUES LIÉS AUX PRESTATAIRES DE SERVICE TIC
Janvier 2024	• RTS - Outils, méthodes, processus et politiques de gestion du risque lié aux TIC (art.15) et Cadre simplifié de gestion du risque lié aux TIC (art.16.3) F A P	• RTS - Classification des incidents liés aux TIC et des cybermenaces (art.18.3) F A P		• RTS – Politique d'utilisation des services TIC supportant des fonctions critiques ou importantes (art.28.10 et art. 28.2) F A P • ITS - Modèles types aux fins du registre d'informations sur les prestataires TIC (art.28.9) F
Juillet 2024	• Orientations communes sur l'estimation des coûts et pertes annuels agrégés occasionnés par des incidents majeurs liés aux TIC (art.11.1) F	• RTS et ITS - Notification des incidents majeurs liés aux TIC et des cybermenaces importantes (art.20) F	• RTS - Tests avancés (art.26) F	• Acte délégué pour préciser les critères pour désigner les prestataires tiers critiques de services TIC (art.31) P • Acte délégué pour préciser le montant des redevances (art.43) P • RTS - Les conditions applicables à la sous-traitance de services TIC qui soutiennent des fonctions critiques ou importantes (art.30.5) F • RTS – La conduite des activités de surveillance des prestataires de services TIC critiques (art.41) F • Orientations sur la coopération et l'échange d'information entre les AES et les autorités compétentes concernant la supervision des prestataires de services critiques (art.32.7) F
JOUE	Juin 2024 • Règlement délégué (UE) 2024/1774 de la commission du 13 mars 2024 - outils, méthodes, processus et politiques de gestion du risque lié aux TIC et le cadre simplifié de gestion du risque lié aux TIC	Juin 2024 • Règlement délégué (UE) 2024/1772 de la commission du 13 mars 2024 - les critères de classification des incidents liés aux TIC et des cybermenaces, fixant des seuils d'importance significative et précisant les détails des rapports d'incidents majeurs		Juin 2024 • Règlement délégué (UE) 2024/1773 de la commission du 13 mars 2024 - la politique relative aux accords contractuels sur l'utilisation de services TIC soutenant des fonctions critiques ou importantes fournis par des prestataires tiers de services TIC Mars 2024 • Règlement délégué (UE) 2024/1505 de la commission du 22 février 2024 – Montant et modalités de paiement des redevances de supervision par les prestataires de services TIC critiques • Règlement délégué (UE) 2024/1505 de la commission du 22 février 2024 - définition des critères de désignation de prestataires tiers de services TIC comme critiques pour les entités financières

2

Vision benchmark de l’état d’avancement du marché

Comment le marché se prépare à DORA ?

Légende

- Maturité / Perception élevée
- Maturité / Perception moyenne
- Maturité / Perception faible

Vision par secteur

	Banque et marchés financiers	Assurance	Asset Management	Third Party Providers
Maturité	↑ *Existence de réglementations au niveau européen sur la Résilience depuis plusieurs années,*	→ *Mise en œuvre tardive des sujets autour des risques digitaux et IT/Cyber à partir de 2021*	↓ *Faible maturité sur toutes les dimensions DORA*	→ *Focus sur les services ICT / Cyber dans une approche de fournisseurs de services*
Perception	→ *Perception d'être "presque prêt" Focus sur les exigences complémentaires apportées par DORA (ex : Stress Test)*	↑ *Analyse d'écarts en cours / terminée pour commencer l'implémentation à temps avec le budget*	↓ *Faible perception des exigences et des besoins de transformation liés à DORA*	↑ *Une attention particulière est portée sur les impacts de DORA compte tenu de la possibilité de supervision par l'UE*
Principaux challenges DORA	• Faire évoluer les dimensions de DORA en surmontant l'approche historique en silo. • L'accent est mis sur les nouvelles exigences de DORA (ex : la stratégie de résilience, la visibilité et la cartographie des services, les tests de cybersécurité).	• Évolution complète de toutes les dimensions liées à DORA. • Investissements importants dans le domaine des risques, de la cybersécurité et des TIC	• Faible maturité sur toutes les dimensions de DORA • Manque de compétences en interne, notamment dans les petites structures • Faible sensibilisation face aux enjeux de DORA entraînant un retard dans le lancement du projet	• Possibilité d'être supervisé par les autorités de l'UE. • Comment faire évoluer les services fournis aux FSI de l'UE tout en maintenant la rentabilité et en générant de nouvelles opportunités

Nous pouvons regrouper les acteurs du marché tous secteurs confondus dans 3 catégories vis-à-vis de leur préparation pour la mise en conformité DORA

« Pioneer organizations »

Cette catégorie d'acteurs a **anticipé** DORA et a commencé son programme de mise en conformité dès la première version du texte

« Mature organizations »

Cette catégorie **dispose déjà d'un socle existant sur la résilience** et a attendu l'entrée en vigueur du règlement pour lancer son programme de transformation DORA

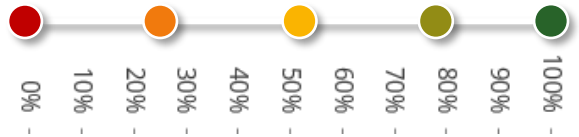
« RTS Waiters »

Cette catégorie a généralement effectué son **analyse d'écarts** avec la réglementation DORA mais **attend les versions finalisées des RTS** pour mettre en œuvre son programme DORA.

Niveau de maturité du marché par rapport aux 5 piliers DORA

L’évaluation du niveau de conformité des institutions financières permet d’identifier des sujets clés à appréhender à travers les 5 piliers de la Réglementation DORA

Les 5 piliers de DORA	*Niveau de conformité des institutions financières**
1 Gestion du risque lié aux TIC	
2 Classification, gestion et notification des incidents majeurs TIC et des cybermenaces	
3 Tests de résilience opérationnelle	
4 Gestion des risques liés aux prestataires de services TIC	
5 Partage d’informations	



Ces niveaux de conformité ont été définis par PwC France sur la base d’accompagnements réalisés pour les institutions financières au profil de risque similaire (Asset Management, Courtiers, Mutuelles…). Le taux de conformité 100% correspond au niveau de conformité DORA qui prend en compte le profil de risque et le principe de proportionnalité conformément à la Réglementation.

3 Les sujets clés à appréhender

DORA - Sujets clés à appréhender

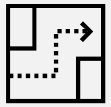
DORA : Les 6 principaux sujets d'échanges DORA avec les entités financières

1. La gouvernance
2. Application du principe de proportionnalité
3. Définition du périmètre et notions de criticité
4. Gestion et notification des incidents TIC et cybermenaces
5. Gestion des risques liés aux prestataires de services TIC
6. Tests de résilience opérationnelle numérique

3.1 Renforcement de la gouvernance

Principe fondamental de la pleine responsabilité de « l'organe de direction » dans la gestion des risques liés aux TIC

« L'organe de direction » **définit, approuve, supervise et est responsable de la mise en œuvre** du dispositif de gestion des risques liés aux TIC. Il est chargé notamment de :



L'établissement et l'approbation de **la stratégie de résilience opérationnelle numérique** y compris la détermination de la limite de tolérance aux risques liés aux TIC en cohérence avec le cadre d'appétit aux risques et sur la base d'une analyse d'impact des perturbations liées aux TIC

La définition claire des **rôles et des responsabilités** avec la mise en place de mécanismes de gouvernance appropriés pour assurer une communication, une coopération et une coordination efficaces et opportunes entre les fonctions liées aux TIC

La mise en place de **politiques** visant à garantir le maintien de **normes élevées en matière de confidentialité, d'intégrité et de disponibilité des données**

La revue **des incidents majeurs liés aux TIC** et de leur incidence, ainsi que des mesures de réponse, de rétablissement et de correction.

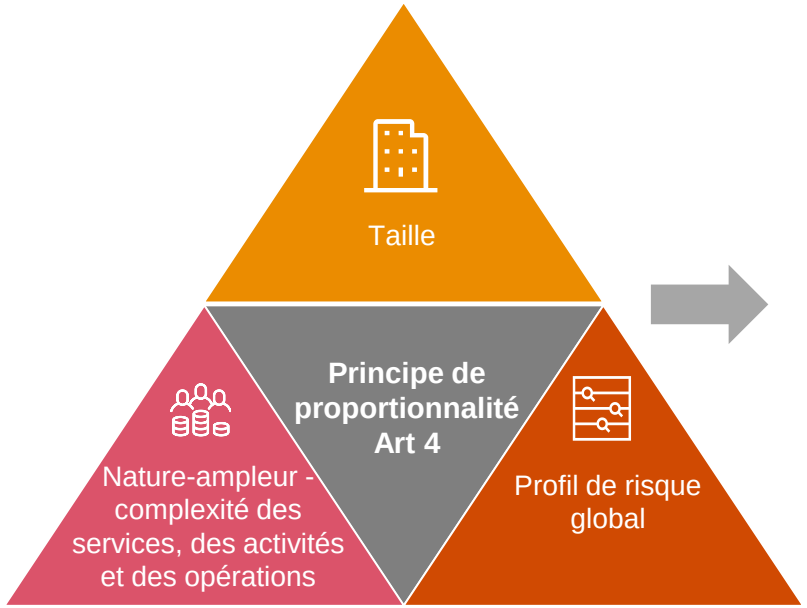
L'approbation, la surveillance et l'examen périodique de la mise en œuvre du **plan de continuité et du plan de réponse et de reprise des activités liés aux TIC**

L'approbation et l'examen périodique de **la politique en matière d'utilisation des services TIC** fournis par des **tiers prestataires de services TIC**, la revue des **accords conclus** et des **modifications apportées** aux contrats existants

3.2 Application du principe de proportionnalité

Principe général de proportionnalité → **Déclinaison du principe de proportionnalité** → **Analyse et application du principe de proportionnalité**

Prise en compte par les entités financières de leurs **caractéristiques suivantes :**



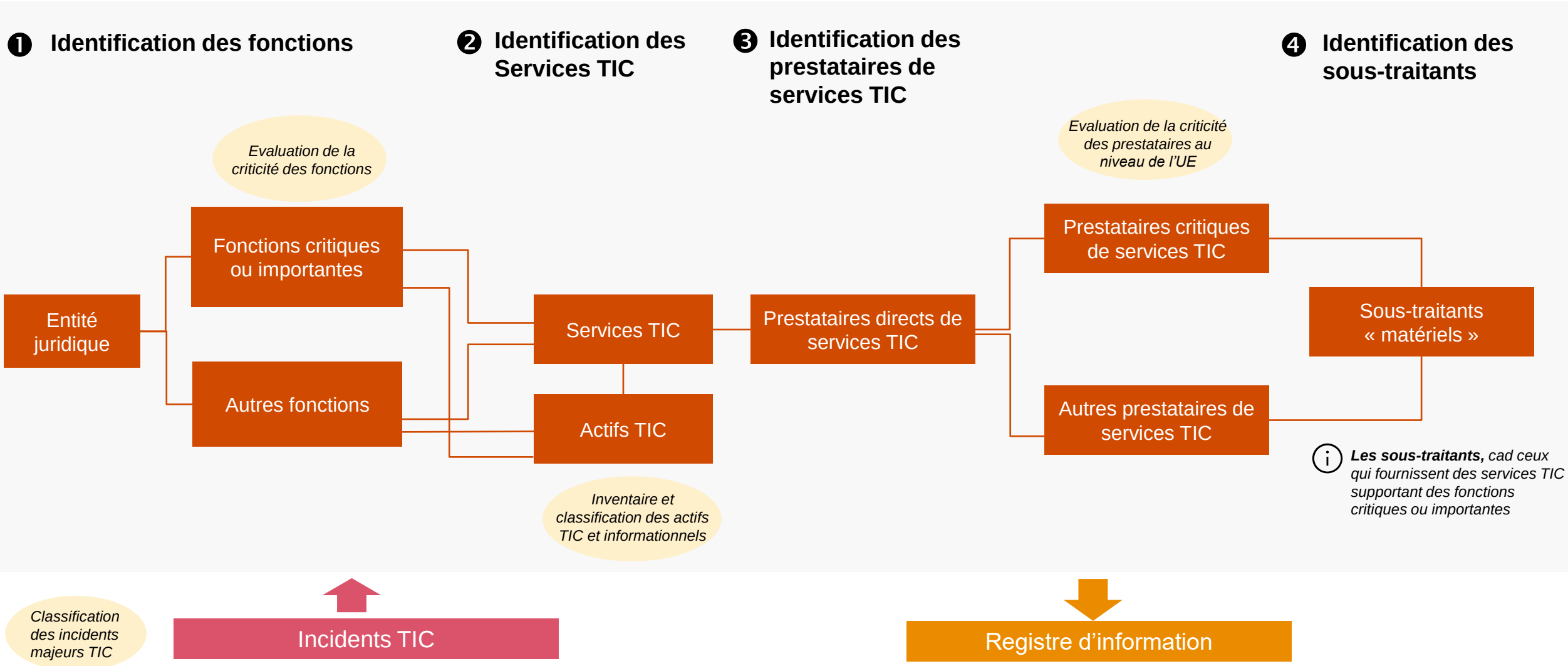
…pour la mise en œuvre des exigences de DORA:

- Gestion des risques TIC
- Gestion des risques liés aux prestataires
- Gestion des incidents TIC
- Tests de résilience opérationnelle numériques

Retour d'expérience

- Analyse préalable à effectuer pour s'assurer de la mise en œuvre de mesures de gestion des risques liés au TIC « proportionnées »
- Analyse couvrant différents angles : nature et échelle des activités, criticité des fonctions et services, projets en cours, environnement et stratégie IT, efficacité des contrôles , posture de sécurité de l'entité, relations de dépendances, type et volume de prestataires de services TIC…;
- Prise en compte des éléments spécifiques tendant à accroître ou réduire la complexité et les risques définis dans les textes de niveau 2
- Documentation de l'application du principe

3.3 Périmètre et notions de criticité (1/2)



3.3 Périmètre et notions de criticité (2/2)

Identification des fonctions critiques ou importantes

Une fonction critique ou importante est une fonction dont l'interruption porterait gravement atteinte :

- à la performance financière de l'entité financière,
- à sa solidité ou à sa continuité de ses services et activités,
- ou dont l'interruption, une anomalie ou une défaillance compromettrait sensiblement le respect continu par une entité financière des conditions et obligations de son agrément, ou de ses autres obligations en vertu de la législation applicable aux services financiers

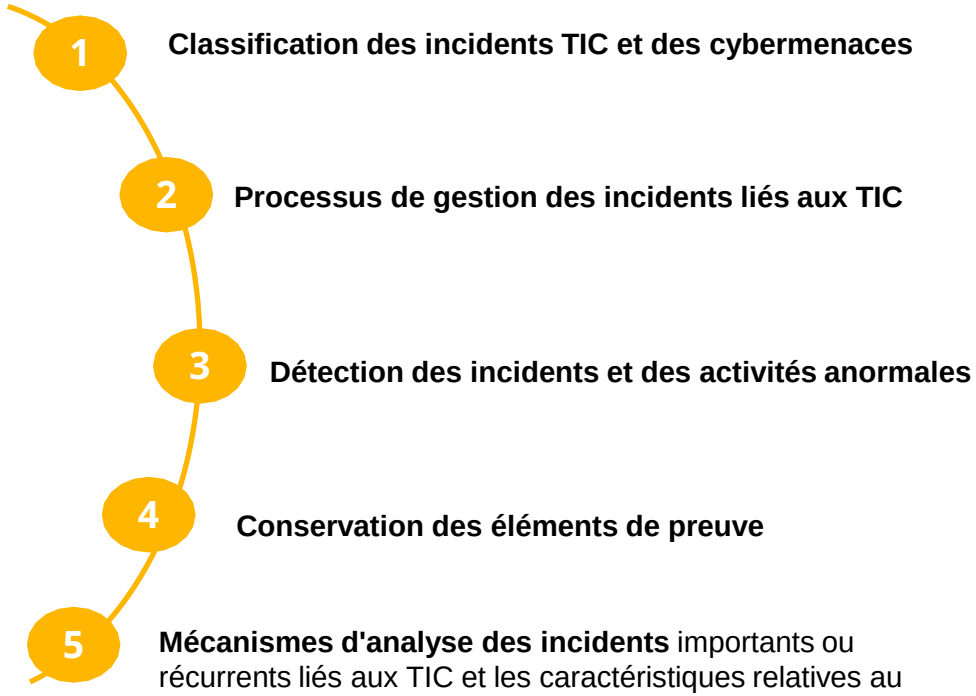
(Article 3, 22 du Règlement DORA)

Retour d'expérience

- Un prérequis structurant pour la mise en œuvre des exigences (mapping des services TIC, des prestataires de services TIC et des sous-traitants matériels, des actifs TIC…)
- Demande de clarification de la notion de « fonction »
- Nécessité de réconcilier une approche Bottom-up (vision départements/processus) avec une vision Top-down (fonctions critiques ou importantes) pour assurer l'évaluation périodique de la criticité des fonctions
- Mise en cohérence avec les cadres existants (externalisation, redressement et résolution) pour un cadre de résilience global
- Nécessité de définir, documenter et valider la méthodologie dans la politique relative à l'utilisation des services TIC qui soutiennent des fonctions critiques ou importantes

3.4 Gestion des incidents TIC

Gestion des incidents liés aux TIC



Retour d'expérience

- Revue des processus en place pour centraliser l'ensemble des incidents (incidents informatiques, de sécurité et cyber et relatifs aux paiements…)
- Nécessité d'aligner la méthodologie de classement des incidents majeurs TIC et des cybermenaces avec les attendus du règlement DORA
- Nécessité de renforcer le dispositif de détection des incidents et activités anormales selon une approche par les risques et par des outils avec des alertes automatisées
- Remontée des vulnérabilités et incidents TIC de la part des prestataires de services TIC à caler pour reporter les incidents majeurs à l'organe de Direction et aux autorités compétentes dans les délais requis.
- Intégration à effectuer des incidents récurrents dans les analyses
- Plan de communication en cas d'incident TIC et en fonction de scénarios à formaliser

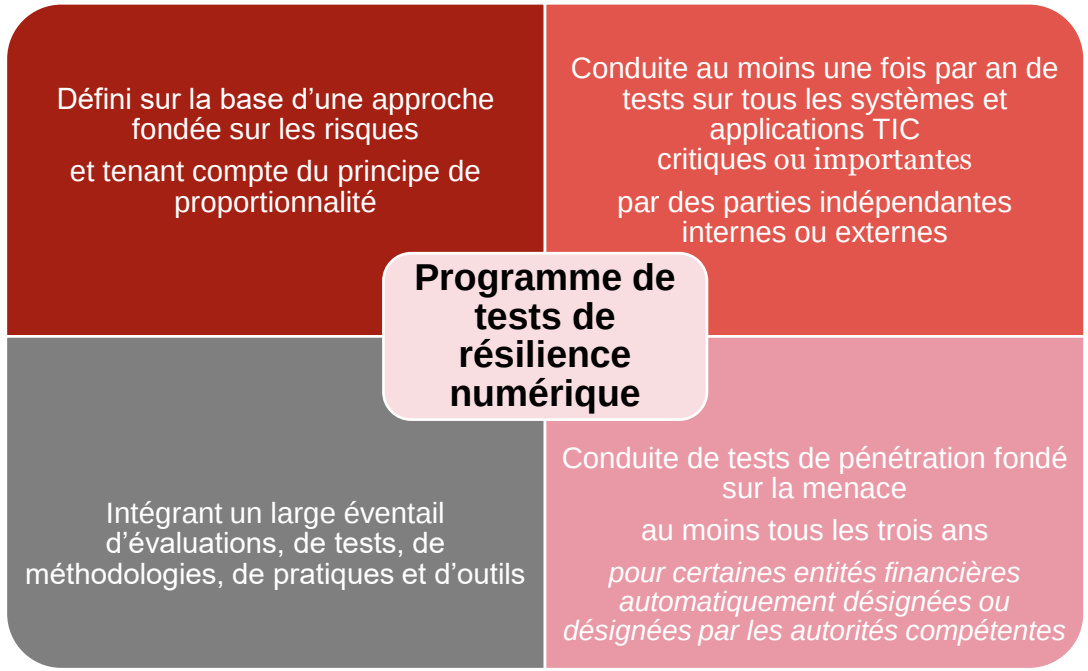
3.5 Gestion des prestataires liés aux TIC

Vue d'ensemble des dispositions relatives à la gestion des risques liés aux prestataires TIC

Retour d'expérience

- Travail important de recensement des services TIC fournis par l'ensemble des prestataires de services TIC, y compris les prestataires intra-groupe et de mise en correspondance avec les fonctions
- Détermination des fonctions critiques ou importantes
- Initiation de la revue des contrats avec les prestataires
- Identification des sous-traitants de services TIC supportant des fonctions critiques ou importantes généralement à initier ainsi que la revue des contrats et la mise en place d'un dispositif de suivi et de surveillance
- Politique d'utilisation des servies TIC supportant des fonctions critiques ou importantes à formaliser
- Stratégies et plans de sortie pour les services TIC supportant des fonctions critiques ou importantes à définir et à tester

3.6 Tests de résilience opérationnelle numérique



Retour d'expérience

- Des tests éparpillés qu'il est nécessaire de rassembler, revoir pour construire un programme global de tests de résilience
- Des tests des capacités de continuité, de restauration et de rétablissement des activités soutenues par les TIC, y compris les activités externalisées à développer
- Des tests des systèmes et applications TIC à effectuer/étendre sur l'ensemble du périmètre des fonctions critiques ou importantes
- Des tests d'intrusion réalisés de manière opportuniste
- Des procédures et des stratégies pour hiérarchiser, classer et résoudre les problèmes mis en évidence au cours des tests à formaliser
- Un suivi des corrections des faiblesses, des défaillances ou des lacunes recensées lors des tests à documenter et systématiser

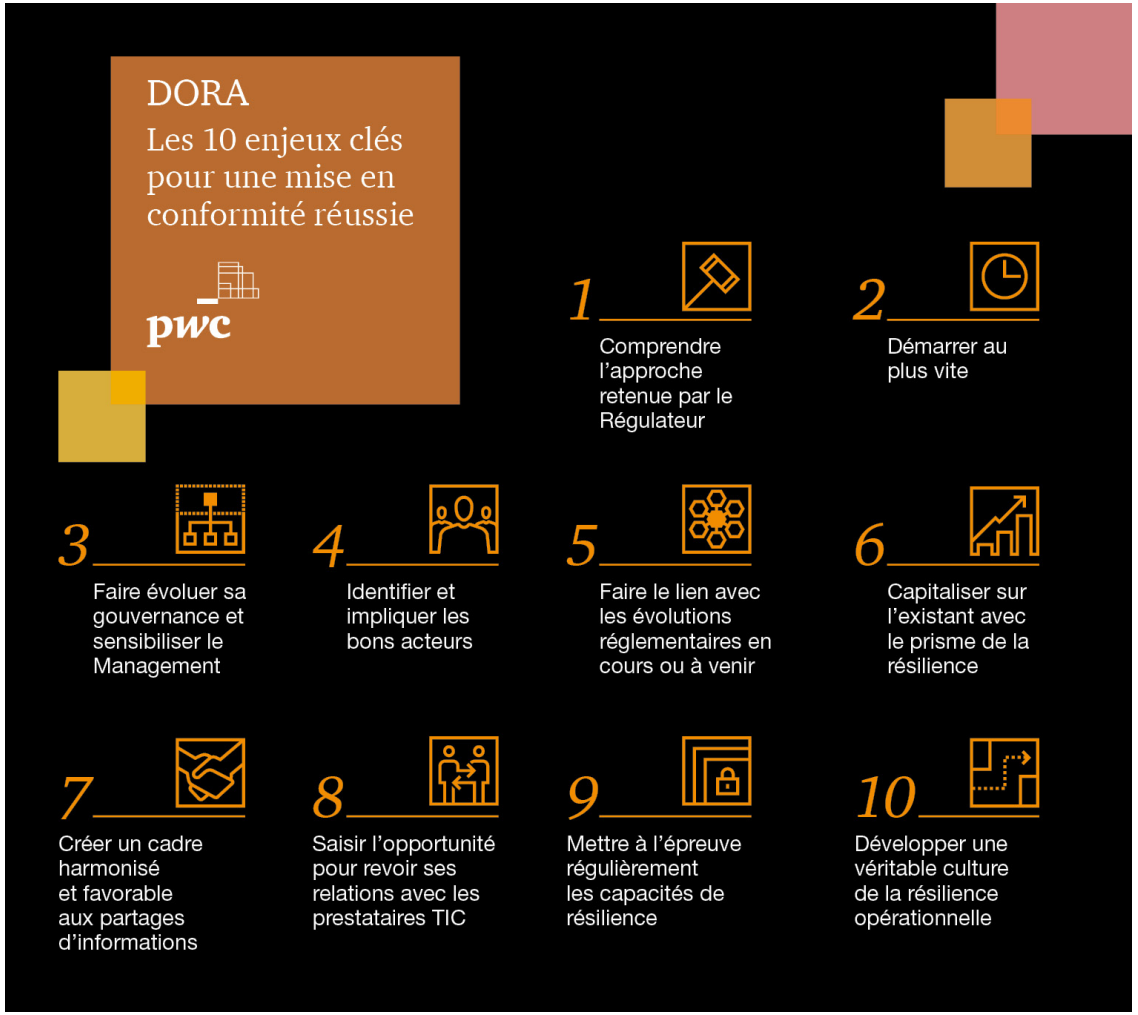
Publications et Prochains évènements

- **Webcast le 17 octobre 2024** : Règlement DORA : quels sont les nouveaux enjeux en matière de risques liés au tiers (TPRM) ?

- Inscrivez-vous dès maintenant via ce lien : https://pwc.to/4dcmkiD

Livre blanc PwC sur le règlement DORA

Disponible sur www.pwc.fr



Merci de votre attention