WEBINAIRE

Pourquoi DORA change-t-il la donne pour la gouvernance du numérique ?

Paris

Le 13/11/2023

WEBINAIRE

Pourquoi DORA change-t-il la donne pour la gouvernance du numérique ?

Le 13/11/2023

Florence Picard	*Administratrice d'une compagnie d'assurance*
Brigitte Dubus	*Administratrice d'une compagnie d'assurance et Associée de Metametris*
David Quantin	*Membre du Comité Exécutif du Groupe Matmut, en charge de la Direction du Numérique et de l'Innovation*
Marc-Antoine Ledieu	*Avocat, spécialiste du droit du numérique*
Hélène Dufour	*Associée de Metametris*

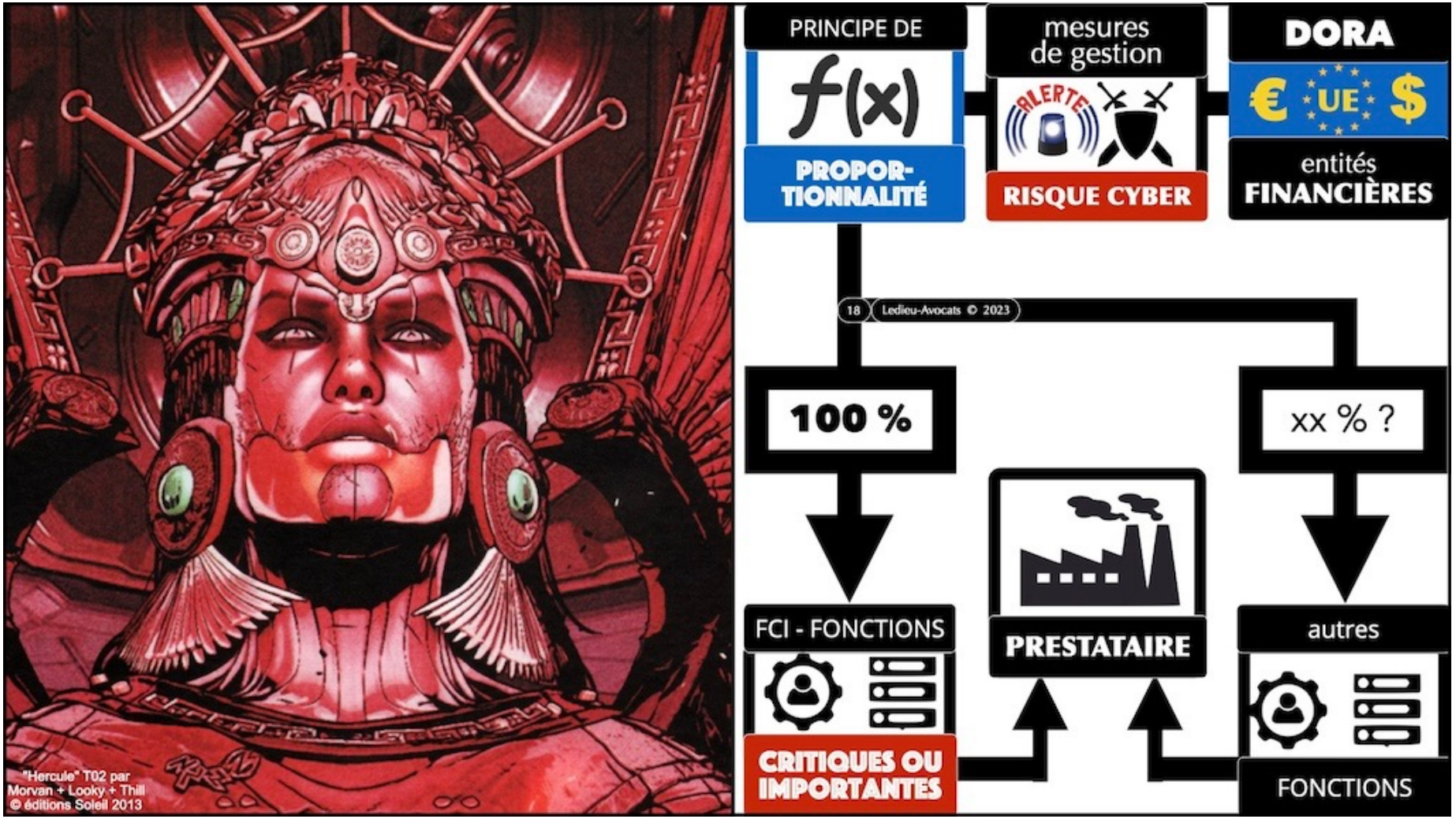
SOMMAIRE

2. Rappel succinct des éléments clés de DORA

2. Rappel succinct des éléments clés de DORA

Institut des ACTUAIRES

2. Rappel succinct des éléments clés de DORA



DORA EST UNE RÉGLEMENTATION PRUDENTIELLE

- DORA impose de nouvelles exigences en matière de résilience opérationnelle numérique pour protéger la solvabilité de l'industrie, elle s'inscrit dans la continuité des orientations EIOPA et des textes ACPR en France.
- DORA renforce et accélère les mesures déjà prises dans les entreprises pour se protéger du risque cyber. En particulier le Conseil d'Administration était déjà impliqué dans la revue de la cartographie des risques opérationnels portée par le CRO,
- Si les orientations EIOPA relèvent de la soft law, DORA est un règlement, d'application immédiate,
- Complémentaire à DORA, la directive UE/2022/2556 amende la directive Solvabilité II en précisant que « les entreprises d'assurances mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement DORA (UE/2022/2554) » https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2556

Nb la « soft law » ou droit mou peut venir des directives internes, du superviseur national ou du superviseur européen, repris par les superviseurs nationaux, elle fait l'objet de contrôles du régulateur national et doit être respectée selon une logique « comply or explain »

OBLIGATIONS DU CA ET MODALITÉ D'ORGANISATION

- Les nouvelles obligations du Conseil d'Administration sont de :
  - Participer à la définition de la stratégie de résilience opérationnelle numérique qui découle du niveau de tolérance au risque,
  - Vérifier que les moyens alloués à la maîtrise du risque sont suffisants
  - Vérifier l'efficacité des dispositifs de maîtrise des risques et le valider dans le cadre d'un rapport
  - Valider les politiques qui encadrent la résilience opérationnelle numérique (1)
- Une pluralité de propriétaires potentiels des risques doivent être impliqués et coordonnés notamment :
  - Les métiers utilisateurs des services de TIC qui doivent définir et recertifier les droits d'accès et contrôler le respect des exigences contractuelles par les tiers,
  - La DSI en charge de mettre en œuvre les mesures de sécurité et contrôler les tiers sur les volets IT - SSI,
  - La conformité en charge de vérifier le respect des réglementations (prévention des conflits d'intérêt…),
  - Le DPO en charge de la conformité au RGPD
  - La Direction Juridique, en charge de la conformité des accords contractuels
- DORA exige la création d'une fonction indépendante de gestion des risques numériques en charge de piloter les contrôles de second niveau
- L'équipe du CRO doit proposer un cadre méthodologique adapté à l'évaluation des risques

(1) PSSI, politique de gestion des risques numériques, politique d'utilisation des services de TIC, politique de continuité d'activité informatique et politique de gestion d'incidents)

LE BESOIN D'UN CADRE MÉTHODOLOGIQUE D'ÉVALUATION DES RISQUES NUMÉRIQUES

- Dans la synthèse de l'enquête déclarative de 2022 sur la gestion de la sécurité des SI des compagnies d'assurance https://acpr.banque-france.fr/sites/default/files/medias/documents/20230223_as_ssi_2022.pdf l'ACPR note que « l'examen des rapports ORSA révèle que très peu d'entreprises d'assurances fournissent des informations relatives aux risques SSI dans l'ORSA et que quand le sujet est abordé, que ces informations sont extrêmement succinctes »,
- Dans le même rapport elle note également que seuls 65% des répondants utilisent les résultats de leur cartographie des risques dans leur processus de décision relatif à l'amélioration de la maîtrise des risques,
- DORA met l'accent sur la nécessité de quantifier les risques numériques ce qui implique de développer des méthodes d'évaluation de ces risques avec le soutien de la Direction des Risques et des actuaires
- La note de méthodologique de l'EIOPA sur les stress tests cyber donne des éléments pour ce faire https://www.eiopa.europa.eu/system/files/2023-07/Methodological%20principles%20of%20insurance%20stress%20testing%20-%20Cyber%20component.pdf

DORA PRÉCISE ET ÉLARGIT LES EXIGENCES DES ORIENTATIONS EIOPA

- Une organisation selon les 3 lignes de défense
- La nomination d'une Fonction gestion des risques numérique en seconde ligne de défense
- Une stratégie de résilience opérationnelle numérique globale couvrant la sécurité et déclinée en stratégie multi-fournisseurs pour les prestataires de TIC,
- En ce qui concerne les tiers DORA ne vise pas la sous-traitance au sens de Solvabilité II mais plus largement l'utilisation des services de TIC avec un focus sur les services qui soutiennent des fonctions critiques ou importantes,
- L'adaptation de tous les accords contractuels,
- La mise en œuvre d'un registre des accords contractuels, aux niveaux solo et consolidé qui intègre des éléments d'appréciation des risques liés aux fonctions supportées, aux services de TIC et aux tiers prestataires de services.

LES MODALITÉS D'IMPLÉMENTATION DES EXIGENCES DE DORA SONT DÉFINIES DANS LES RTS

- 4 RTS ont été publiées en mode draft et soumises à consultation en juin 2023, leur version définitive devrait paraître le 17 janvier 2024
  - RTS sur le cadre de gestion des risques liés aux TIC,
  - RTS sur la politique d'utilisation des services de TIC qui soutiennent des fonctions critiques ou importantes,
  - RTS sur les critères de classification des incidents liés aux TIC,
  - RTS sur le registre des informations relatives aux accords contractuels avec des tiers prestataires de services TIC.
- Une deuxième tranche de RTS à paraître en mode draft d'ici fin 2023 et en mode définitif le 17 juillet 2024 : couvrira les domaines suivants :
  - RTS sur l'estimation des coûts/pertes agrégés causés par des incidents TIC majeurs,
  - RTS sur les modalités de reporting des incidents majeurs liés aux TIC,
  - RTS sur le cadre pour les tests d'intrusion basés sur les menaces,
  - RTS sur les clauses relatives aux accords contractuels avec les prestataires de services de TIC.

LE TÉMOIGNAGE DE LA MATMUT

6. Avancées du rapport de réexamen du cadre de gestion des risques numériques par rapport à l'ORSA

UN RAPPORT DE CONTRÔLE DÉDIÉ AUX RISQUES NUMÉRIQUES (SOURCE RTS N°1)

A tenir à disposition des régulateurs à leur demande il doit intégrer les éléments suivants :

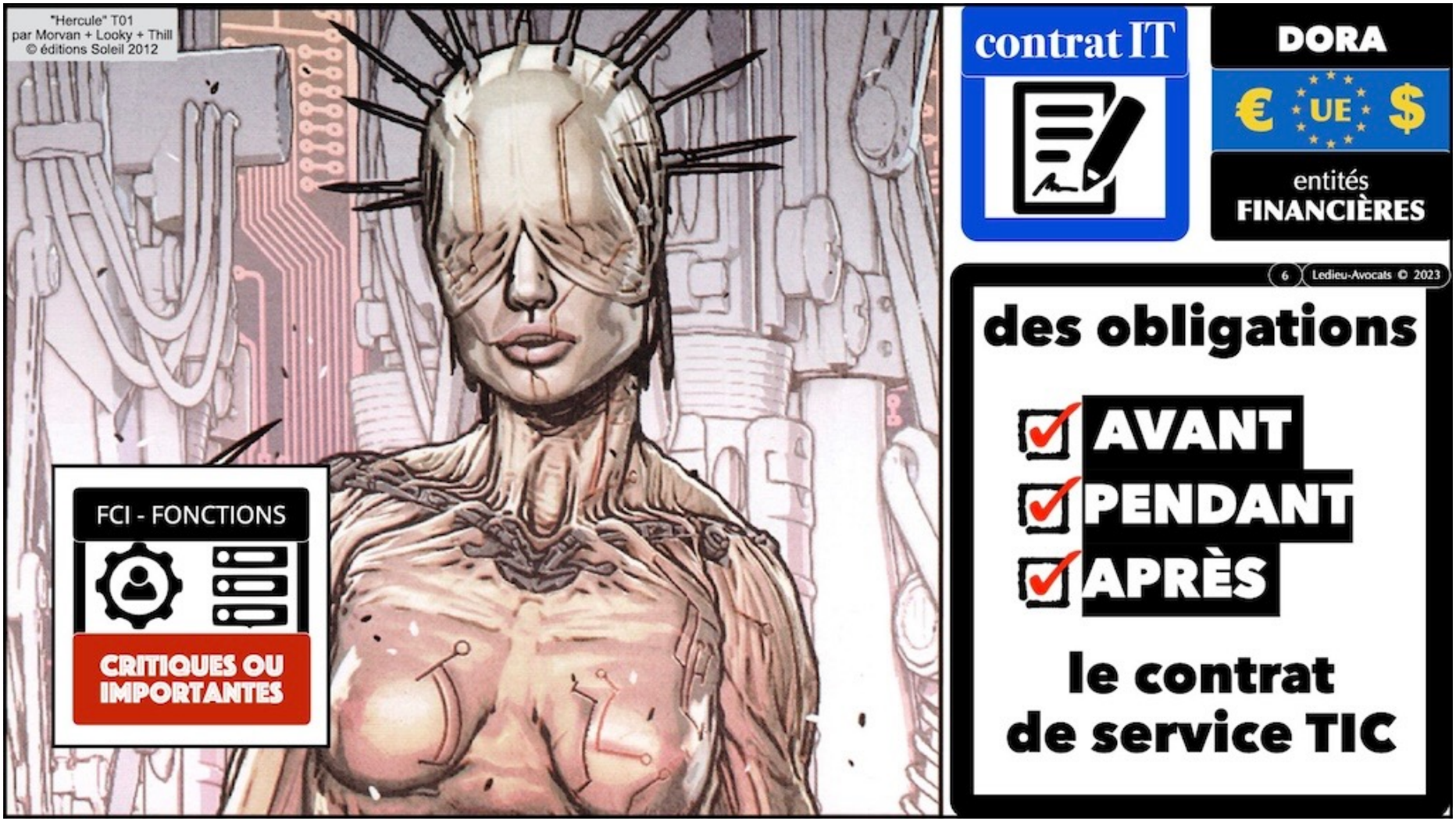
- Une description du contexte décrivant la nature l'échelle et la complexité des services, activités et opérations, l'organisation et les fonctions critiques ou importantes,
- Une description de la dépendance par rapport à des services de TIC développés en internes ou par des tiers et de l'impact de leur indisponibilité totale ou de leur dégradation sévère sur les fonctions critiques ou importantes,
- Un résumé de l'identification des risques numériques actuels et potentiels à court terme, du paysage de la menace et de l'efficacité des contrôles,
- Un résumé des changements depuis le dernier rapport et de leur impact,
- Un résumé des constatations et une auto-évaluation de la sévérité des faiblesses et des déficiences identifiées,
- Les mesures de remédiation identifiées, leur date d'implémentation et leur suivi,
- Les conclusions du rapport et les développements ultérieurs prévus.

NB : a priori la RTS N°1 ne fait pas référence aux résultats des stress tests cyber EIOPA pour le contenu de ce rapport, on peut donc supposer qu'ils seront à documenter dans l'ORSA

L'ÉVOLUTION DES RELATIONS CONTRACTUELLES AVEC LES TIERS PRESTATAIRES DE TIC

Marc-Antoine Ledieu

7. Mise à jour des accords contractuels



7. Mise à jour des accords contractuels

Institut des ACTUAIRES

7. Mise à jour des accords contractuels

DORA

€ UE $

entités FINANCIÈRES

contrat IT

l'évaluation préliminaire du risque de concentration

FCI - FONCTIONS

CRITIQUES OU IMPORTANTES

DORA article 29.1 — 12 — Ledieu-Avocats © 2023

"Lorsqu'elles procèdent à **l'identification et à l'évaluation des risques [de concentration]**, les entités financières déterminent si la conclusion envisagée d'un [contrat de] services TIC qui soutiennent des **FONCTIONS CRITIQUES OU IMPORTANTES** déboucherait sur" :

☑ "conclusion d'un contrat avec un prestataire dont les **services ne sont pas facilement substituables**

☑ plusieurs [contrats] **avec le même prestataire ou avec des prestataires étroitement liés**"

"Hercule" T03 par Morvan + Looky + Thill © éditions Soleil 2017

Institut des ACTUAIRES

7. Mise à jour des accords contractuels

DORA

€ UE $

entités **FINANCIÈRES**

contrat IT

FCI - FONCTIONS

CRITIQUES OU IMPORTANTES

1/3 - SERVICES CRITIQUES OU IMPORTANTS

➡ DORA article 30.3

13 Ledieu-Avocats © 2023

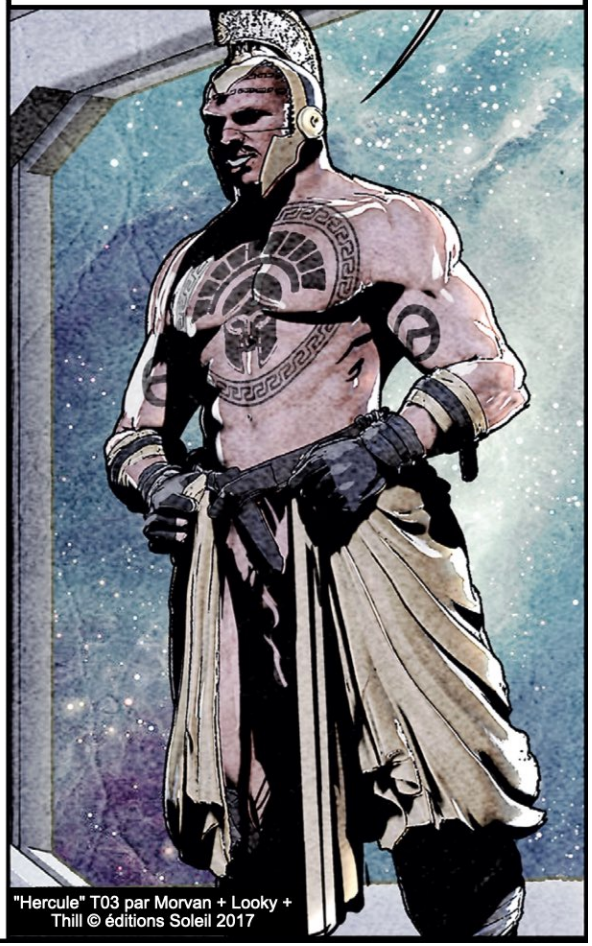
(a) **descriptions complètes des niveaux de service**, y compris leurs mises à jour et révisions , **assorties d'objectifs de performance quantitatifs et qualitatifs précis** dans le cadre des niveaux de service convenus, afin de … prendre dans les meilleurs délais, sans retard injustifié, des mesures correctives appropriées lorsque les niveaux de service convenus ne sont pas atteints;

(b) **délais de préavis et obligations de notification** du prestataire à l'entité financière, y compris la notification **de tout développement susceptible d'avoir une incidence significative sur la capacité du prestataire à fournir les services** … de manière efficace conformément aux niveaux de service convenus;

(c) **obligation pour le prestataire de mettre en œuvre et de tester des plans d'urgence** et de mettre en place des mesures, des outils et des politiques de sécurité des TIC qui fournissent un niveau approprié de sécurité en vue la prestation de services sûre par l'entité financière…;

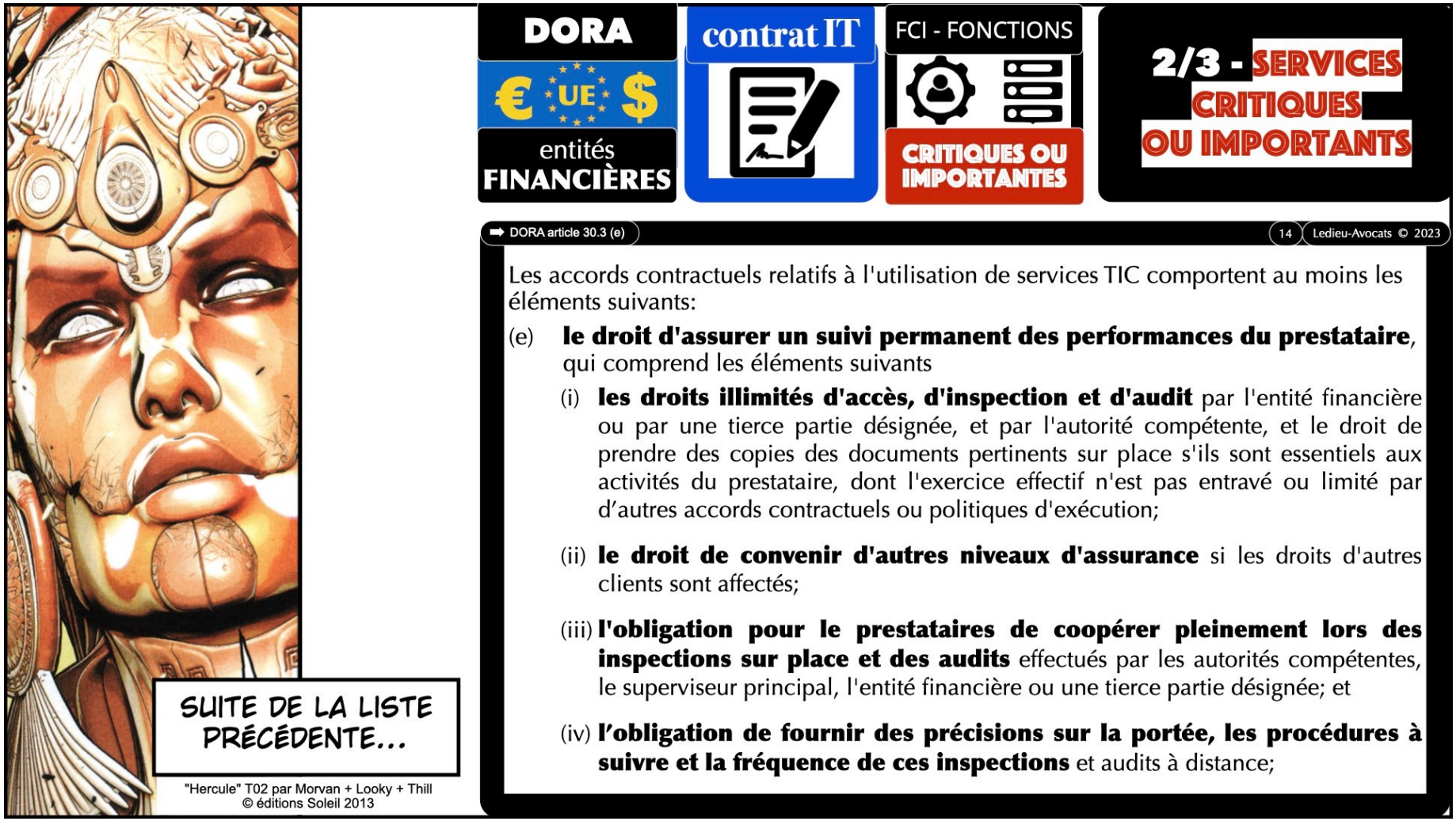
(d) **l'obligation pour le prestataire de participer et de coopérer pleinement au test de pénétration fondé sur la menace**…;

DES MENTIONS EN PLUS POUR LES **SERVICES CRITIQUES OU IMPORTANTS** ?



"Hercule" T03 par Morvan + Looky + Thill © éditions Soleil 2017

7. Mise à jour des accords contractuels



Institut des ACTUAIRES

7. Mise à jour des accords contractuels

Institut des ACTUAIRES

7. Mise à jour des accords contractuels

DORA

€ UE $

entités **FINANCIÈRES**

FCI - FONCTIONS

CRITIQUE OU IMPORTANTE

contrat IT

3/3 - services CRITIQUES OU IMPORTANTS

DORA article 30.3 (f) — 16 — Ledieu-Avocats © 2023

"Les accords contractuels relatifs à l'utilisation de services TIC comportent au moins les éléments suivants:

(f) **les stratégies de sortie, en particulier la fixation d'une période de transition adéquate obligatoire** :

(i) **au cours de laquelle le prestataire continuera à fournir les fonctions ou services TIC concernés** en vue de réduire le risque de perturbation au niveau de l'entité financière ou d'assurer sa résolution et sa restructuration efficaces ;

(ii) **qui permet à l'entité financière de migrer vers un autre prestataire ou de recourir à des solutions en interne adaptées à la complexité du service fourni**"

EXIGENCES RELATIVES À LA GESTION DE LA RELATION AVEC LES PRESTATAIRES

A la conclusion du contrat

- Détermination du niveau de criticité de la solution et si elle soutient une fonction critique ou importante,
- Evaluation des risques notamment d'indisponibilité du prestataire, de concentration et de conflit d'intérêt,
- Evaluation du dispositif de sécurité du prestataire,
- Evaluation du dispositif de résilience opérationnelle du prestataire notamment définition claire des responsabilités en matière de sauvegarde des données,
- Evaluation du SLA du prestataire,
- Elaboration d'un plan de réversibilité.

Pendant l'exécution du contrat

- Suivi de la performance par rapport au SLA,
- Notification des changements de la part du prestataire et suivi de leur mise en œuvre,
- Le cas échéant exercice du droit d'audit,
- Suivi du dispositif de sécurité du prestataire en fonction de l'évolution de la menace notamment de la réalisation de pentests par le prestataire
- Assistance de la part du prestataire en cas d'incident cyber,
- Réévaluation des risques.

A la résiliation du contrat et pendant la phase post-contractuelle

- Modalités de résiliation en cas de manquement du prestataire à ses obligations ou en cas d'évolution du service susceptible d'avoir des impacts sur la capacité du client à assumer ses propres responsabilités pour des fonctions critiques ou importantes,
- Activation du plan de réversibilité
- Accompagnement de la part du prestataire à l'activation du plan de réversibilité.
- Exercice des droits d'accès, de récupération et de restitution des données.

Le client reste responsable du service de son prestataire et sa responsabilité peut être recherchée en cas d'incident cyber touchant son prestataire et ayant un impact sur les données de ses clients

LES ÉLÉMENTS STRUCTURANTS QUI DOIVENT FIGURER DANS TOUS LES CONTRATS

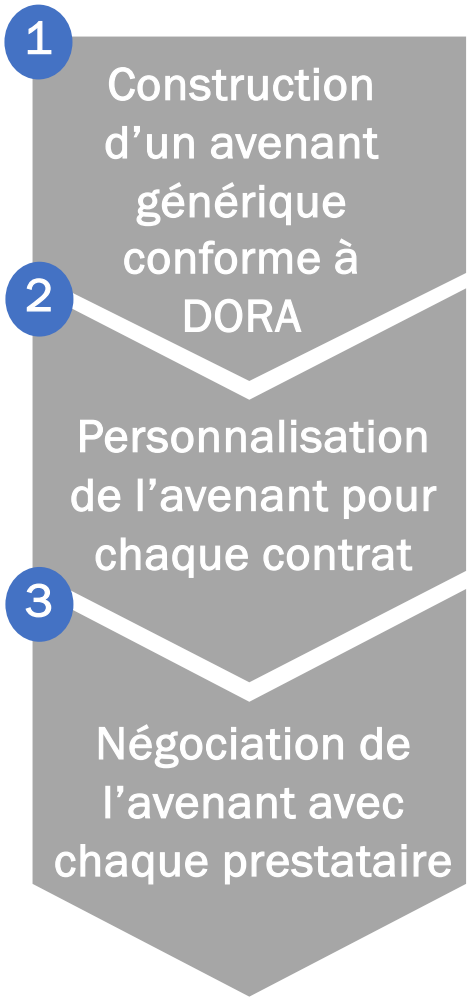
Eléments devant figurer dans tous les contrats

- Description des services assurés précisant s'ils soutiennent une fonction critique ou importante,
- Définition des lieux d'exercice de la prestation et de stockage des données,
- Description des mesures de sécurité,
- Définition des droits et conditions de résiliation
- Clause de réversibilité avec garantie d'accès, de récupération et de restitution des données à la fin de l'accord contractuel ou en cas de cessation d'activité du prestataire,
- Coopération du prestataire avec les autorités et maintien du service en cas de résolution de l'institution financière,
- Description des niveaux de services (SLA) et des engagements de performance,
- Assistance du prestataire en cas d'incident cyber.

Eléments devant figurer dans les contrats de prestations soutenant des fonctions importantes ou critiques

- Notification par le prestataire de tout changement ayant un impact sur le service,
- Obligation pour le prestataire de mettre en œuvre et de tester des plans d'urgence et de poursuite d'activité,
- Coopération du prestataire aux tests de pénétration fondé sur la menace effectués par l'entité,
- Droits illimités d'accès, d'inspection et d'audit par l'entité ou par une tierce partie désignée,
- Engagement de résultat sur les niveaux de service et suivi de la performance,
- Liste des sous-traitants contribuant au service et engagement du prestataire à s’assurer que ses sous-traitants respectent les engagements pris au titre de l’accord contractuel.

7. Mise à jour des accords contractuels

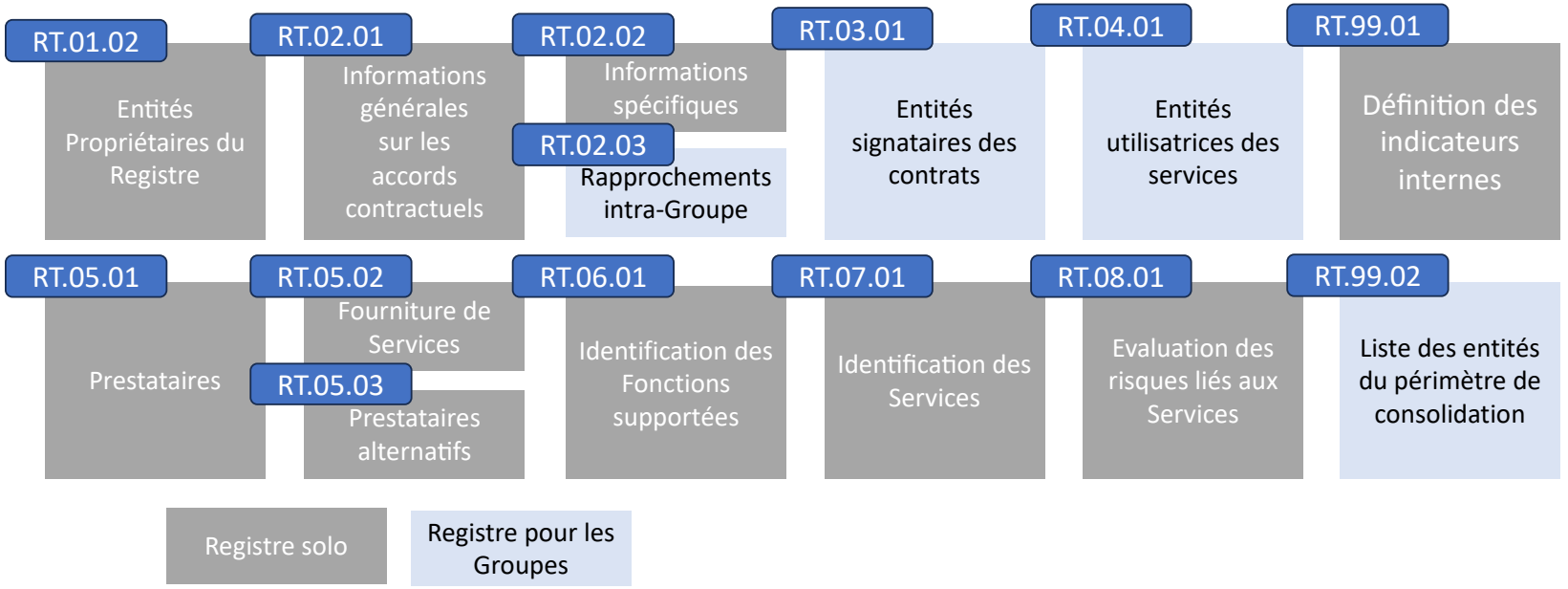


- Tous les contrats avec les prestataires de services de TIC vont devoir être mis en conformité avec des clauses plus contraignantes pour les prestataires de services qui soutiennent des fonctions critiques ou importantes,
- Pour des questions d'efficacité cette mise en conformité peut se faire par un avenant générique défini par l'entité
- L'avenant générique devra être personnalisé pour chaque prestataire en fonction :
  - Du caractère critique ou important ou non des fonctions supportées par le service,
  - Des clauses du contrat initial,
- Chaque prestataire fera ensuite ses retours par rapport à l'avenant type et il faudra négocier les clauses.

8. Registre des accords contractuels

A ÉLABORER AUX NIVEAUX SOLO ET CONSOLIDÉ

Le registre se présente sous la forme d'une base de données relationnelle avec 14 tables et une centaine de champs :



AUX NIVEAUX SOLO ET CONSOLIDÉ

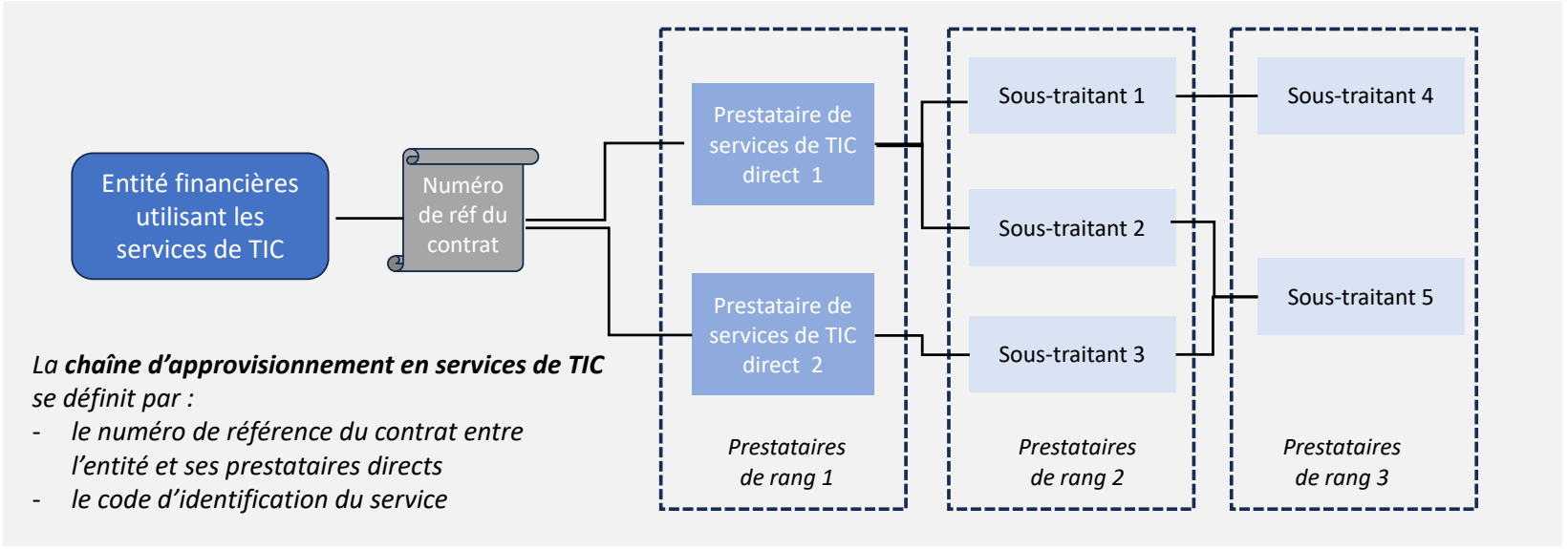
Des informations sont à collecter au niveau des fonctions, des services et des tiers notamment :

Informations sur les fonctions
Identifiant de la fonction
Nom de la fonction
Evaluation de la criticité ou de l'importance de la fonction
Justification de la criticité ou de l'importance de la fonction
La fonction est-elle considérée comme critique en termes de disponibilité ?
RTO de la fonction
RPO de la fonction
Impact d'une interruption de la fonction

Informations sur les services
Identifiant du service
Nom du service
Description du service
Existence d'un plan de réversibilité
Possibilité de réintégration du service
Impact d'une interruption du service
Niveau de sensibilité des données stockées par le tiers prestataire de service

Informations sur les tiers prestataire de service
Nom du prestataire de service
Pays du siège social du tiers prestataire de services
Adresse enregistrée du tiers prestataire de services
Appartenance du prestataire à une alliance ou un groupe
Nom de la société mère ultime du tiers prestataire de service
Le tiers prestataire de service est-il un prestataire intra-groupe ?
Rang du prestataire de service
Nom du prestataire de service de TIC sous-traité au prestataire de rang 1
Nom du prestataire de service alternatif
Pays de résidence du tiers prestataire de service alternatif

IDENTIFICATION DE TOUTE LA CHAINE D'APPROVISIONNEMENT EN TIC



*La **chaîne d'approvisionnement en services de TIC** se définit par :*

- *le numéro de référence du contrat entre l'entité et ses prestataires directs*
- *le code d'identification du service*

LES QUESTIONS QUI SE POSENT:

Le sujet est par nature transverse et nécessite une comitologie adaptée.

Quelques premières questions se posent :

- Quel rattachement pour la fonction indépendante de gestion des risques numériques?
- Quelles sont les fonctions critiques ou importantes au sens de DORA ?
- Comment mener le projet de mise à niveau des accords contractuels avec les prestataires?
- Quel rôle pour l'actuaire ?
  - méthodologie de mesure de risque
  - quantification du risque
  - études d'impact et scénarios
  - contribution à la stratégie
  - ...

10. Sources bibliographiques

Texte du règlement :
https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020PC0595
Orientations EIOPA sur la sécurité et la gouvernance des TIC:
https://acpr.banque-france.fr/sites/default/files/media/2021/07/02/20210702_notices_orientations_aeapp.pdf
Orientations EIOPA sur l'externalisation vers des prestataires de services en nuage :
https://acpr.banque-france.fr/sites/default/files/media/2020/07/22/annexe_orientations_aeapp.pdf
Principes méthodologique pour les stress tests cyber des assureurs :
https://www.eiopa.europa.eu/system/files/2023-07/Methodological%20principles%20of%20insurance%20stress%20testing%20-%20Cyber%20component.pdf
Synthèse de l'enquête déclarative ACPR de 2022 sur la gestion de la sécurité des SI des compagnies d'assurance
https://acpr.banque-france.fr/sites/default/files/medias/documents/20230223_as_ssi_2022.pdf

CONTACTS

Marc-Antoine Ledieu Ledieu & Avocats ma@ledieu-avocats.fr
Auteur du blog en BD :
https://technique-et-droit-du-numerique.fr/dora-03-resilience-operationnelle-secteur-financier-la-menace-et-ses-definitions-legales/

Hélène Dufour Metametris helene.dufour@metametris.com
Auteur de l'article : le règlement DORA change-t-il la donne en matière de gouvernance des TIC?
https://blog-conformite.esbanque.fr/le-reglement-dora-change-t-il-la-donne-en-matiere-de-la-gouvernance-des-risques-lies-aux-technologies-de-linformation-et-de-la-communication/