Résilience opérationnelle numérique – DORA

Convictions et enjeux

novembre 2023

BEAM & SAGALINK

ALETELA

Sommaire

01 Contexte

02 DORA & Services TIC

03 Calendrier réglementaire

04 Impacts clés

05 Objectifs & démarche

BEAM & SAGALINK

ALETELA

01

Contexte

BEAM
& SAGALINK

ALETELA

Contexte (1/2)

Contexte

À l'ère numérique actuelle, les institutions financières sont particulièrement **vulnérables aux cyberattaques** en raison de **la nature sensible de leurs données et de leurs transactions**. Par conséquent, elles sont tenues **d'investir massivement dans la sécurité informatique** pour **se protéger contre ces menaces croissantes**. La réglementation Digital Operational Resilience Act (DORA) s'inscrit dans une **nécessité de tenir compte du risque lié aux Technologies de l'Information et de la Communication** (TIC) dans le contexte d'un système financier mondial fortement **interconnecté.**

Ci-dessous sont listées **les principales formes** d'une cyberattaque :

Phishing

Envoi de **mails** ou de **messages frauduleux** pour **tromper les utilisateurs** en leur faisant **divulguer des informations sensibles**, telles que des identifiants de connexion ou des informations financières

Ransomware

Chiffrement des données par des logiciels **malveillants** les rendant **inaccessibles**. Une **rançon** est généralement demandée **en échange de la clé de déchiffrement**

Vol d'identité

Usurpation de l'identité d'une personne ou d'une organisation pour **accéder à des comptes ou à des informations sensibles**

Déni de Service Distribué

Attaque visant à **rendre inaccessible** un serveur via un envoi de multiples requêtes jusqu'à le **saturer** ou par l'exploitation de faille de sécurité afin de provoquer **une panne** ou un fonctionnement fortement dégradé du service

Malware

Attaque visant à **infecter les systèmes** pour **voler des données**, **endommager des fichiers** ou permettre aux attaquants de **prendre le contrôle des machines**. Cette attaque se fait à travers des **logiciels malveillants** tels que les **virus**

Rétro-ingénierie

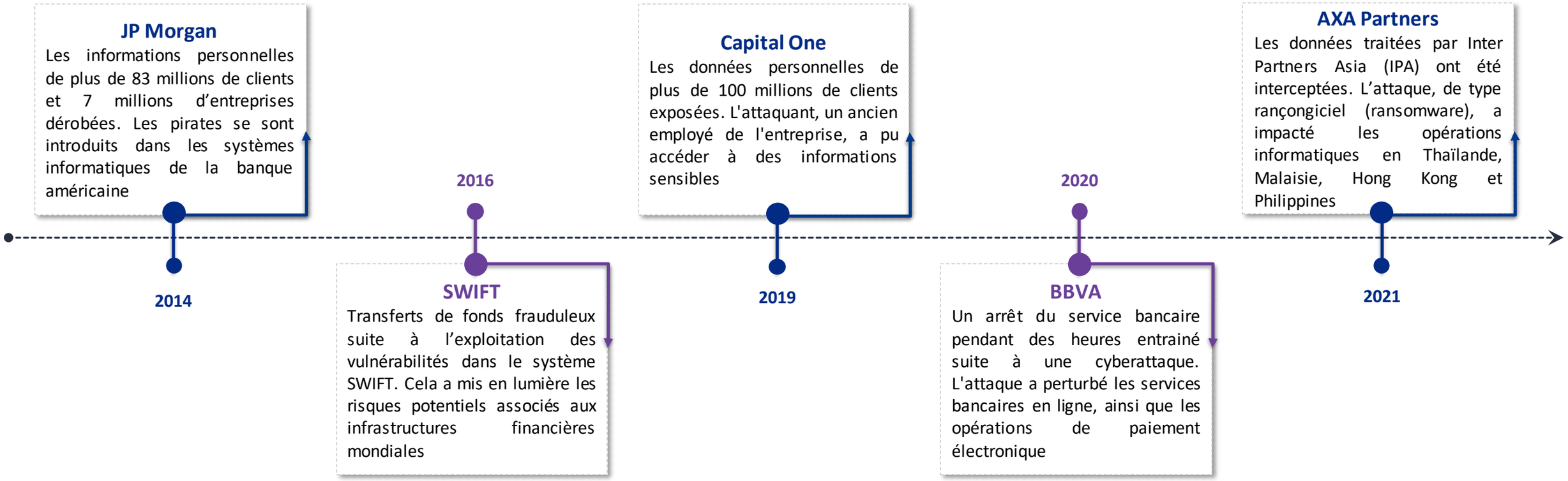
Analyse des logiciels ou du matériel afin **d'identifier les failles et les vulnérabilités cachées**

Ces formes de cyberattaques sont en **évolution continue** dans la mesure où les attaquants continuent à développer de **nouvelles techniques** pour exploiter les **vulnérabilités des systèmes et des utilisateurs**.

Contexte (2/2)

50% des entreprises françaises, dont **22% dans le secteur financier**, déclarent avoir **été victimes d'une cyberattaque**. Les **22% comprennent 70% d'établissements bancaires.**

Ci-dessous sont présentés quelques exemples **des principales cyberattaques dans le domaine financier** depuis 2014 :



02

DORA & Services TIC

BEAM
& SAGALINK

ALETELA

Définitions

DORA

Le Règlement européen DORA[1] est entré en vigueur le 17 janvier 2023 et a pour objectif de **renforcer la résilience opérationnelle numérique** dans le secteur financier.

Il définit la résilience opérationnelle numérique comme étant « ***la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelle*** *en assurant* ***directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC****, l'intégralité des capacités liées aux TIC nécessaires pour* ***garantir la sécurité des réseaux et des systèmes d'information*** *qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbations* ».

Tous les types **d'entités financières européennes** doivent **mettre en œuvre** ce nouveau Règlement et **être conformes à ses exigences à partir du 17 janvier 2025.**

Les Autorités Européennes de Supervision (AES) sont en train de **développer les standards techniques** qui détaillent certaines **des exigences de DORA**. Le premier lot de standards doit être finalisé fin 2023.

Afin de **garantir que les institutions financières** et **les prestataires de services essentiels aux marchés financiers** soient **mieux préparés** à faire face **aux risques liés à la cybersécurité** et à **d'autres incidents opérationnels**, la réglementation DORA permet de :

1. **Harmoniser** les **exigences clés** en matière de **résilience opérationnelle numérique** pour **toutes les entités financières**
2. **Consolider** et **mettre à niveau les exigences en matière de risque** lié aux TIC dans le cadre des exigences en matière de risque opérationnel
3. **Atteindre une résilience opérationnelle** numérique élevée
4. **Limiter les risques systémiques** potentiellement induits par les prestataires critiques de TIC

[1] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, « Digital Operational Resilience Act » (DORA)

Champs d'application

Entités concernées

- Les sociétés de gestion, les gestionnaires de fonds d'investissement alternatifs
- Les entreprises d'assurance et de réassurance, les intermédiaires d'assurance et de réassurance, les institutions de retraite professionnelle
- Les agences de notation de crédit, les administrateurs d'indices de référence critiques, les prestataires de services de financement participatif, référentiels des titrisations

- Les établissements de crédit, de paiement, de monnaie électronique
- Les entreprises d'investissement, les dépositaires centraux de titres, les contreparties centrales, les plates-formes de négociation
- Les référentiels centraux, les prestataires de services de communication de données

- De plus, dès lors qu'une société **fournit des services TIC** à une entité financière, cette société est **directement concernée en tant que prestataire par les exigences** de la **réglementation DORA**.
- DORA définit les « *services TIC* » comme **étant « *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*. »

Piliers de DORA

La résilience opérationnelle des entités financières repose sur **5 principaux piliers :**

Gestion des risques liés aux TIC

Disposer d'un cadre de gestion des risques liés aux TIC avec un ensemble de principes et d'exigences solides, complets et bien documentés. L'objectif étant d'appréhender les risques de manière rapide et efficace afin de garantir un niveau de résilience opérationnelle numérique élevé

Gestion, classification et notification des incidents TIC

Définir et mettre en œuvre un processus de gestion des incidents liés aux TIC dans le but de détecter, gérer et notifier les incidents liés aux TIC

Test de résilience opérationnelle numérique

Évaluer, tester et mettre en place des méthodologies afin de recenser les faiblesses, les défaillances et les lacunes en matière de résilience opérationnelle numérique

Gestion des risques liés aux prestataires tiers de services TIC

Garantir un contrôle efficace des fournisseurs tiers de services TIC en appliquant des principes de surveillance des risques, en intégrant des clauses contractuelles clés et en établissant un cadre de supervision pour les fournisseurs de services TIC critiques

Partage d'informations

Mettre en place un dispositif de partage d'informations et de renseignements sur les cybermenaces. L'objectif de ce partage d'informations est d'améliorer la résilience opérationnelle numérique

03

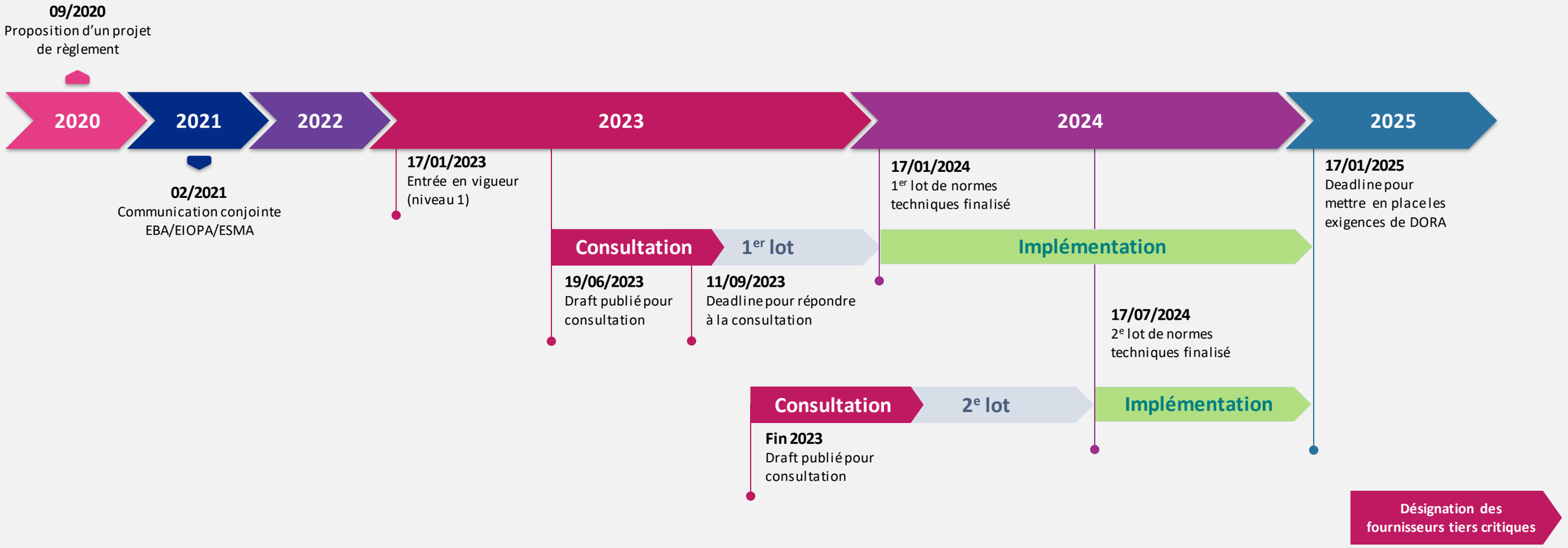
Calendrier réglementaire

BEAM
& SAGALINK

ALETELA

Calendrier réglementaire

Le calendrier réglementaire de DORA ne laisse qu'un **temps très limité** pour **implémenter ses exigences**, dont certaines doivent être détaillées **dans des standards techniques qui ne seront finalisés qu'en 2024**.



Le nombre de **cyberattaques** au sein des entités financières **a fortement augmenté depuis le second semestre 2022**(*), par conséquent, la date limite prévue au **17/01/2025**, pour la mise en application de la réglementation DORA, est **peu susceptible d'être reportée.**

(*) Rapport de l'ESMA - *Trends, Risks and Vulnerabilities, No. 2, 2023*

04

Impacts clés

BEAM & SAGALINK

ALETELA

Impacts clés (1/2)

DORA impactera largement les organisations et processus, au-delà des domaines de la cybersécurité et de la résilience opérationnelle

Cybersécurité	• Une analyse d'impact est nécessaire pour déterminer les éléments de cybersécurité et du cadre de gestion des risques TIC qui doivent être renforcés pour répondre aux exigences de DORA • Des tests avancés des systèmes et processus sur la base de tests de pénétration fondés sur la menace devraient être mis en œuvre selon une méthodologie réglementaire spécifique (en cours de développement par les AES)
Résilience opérationnelle	• Une analyse des incidences sur les activités (Business Impact Analysis, [illegible]) des perturbations doit être réalisée sur la base de critères qualitatifs et quantitatifs • Des plans de continuité des TIC doivent être mis en place [illegible] (y compris des scenarios de cyber-attaques) • Des plans de communication de crise sont [illegible] internes et externes, sous la responsabilité d'une personne désignée à cet effet.
Notification des incidents	• Les incidents majeurs liés [illegible] doivent être déclarés [illegible] compétent • Une classification [illegible] de la sévérité des incidents liés aux TIC, et une procédure de notification spécifique doivent être mis en œuvre
Gouvernance et processus	• La gouvernance et les processus de gestion des TIC devraient être renforcés : cadre de gestion des risques TIC, stratégie de résilience opérationnelle numérique, politique de continuité d'activité des TIC, politique de conduite du changement des TIC, ... • Les organes de direction (conseil d'administration, direction générale) doivent définir, valider et superviser le cadre de gestion du risque lié aux TIC et allouer des budgets et ressources appropriés pour sa mise en œuvre

Impacts clés (2/2)

Prestataires de services TIC	• Une stratégie en matière de risques liés aux prestataire tiers de services TIC doit être définie et mise en œuvre • Les processus de sélection de prestataires doivent être renforcés, avec notamment une évaluation préalable des risques (y compris de concentration et liés à la sous-traitance), et des diligences requises (‘due diligence’) • Les contrats de service doivent incluront les clauses obligatoires requises par la réglementation, des dispositions de niveaux de services détaillés avec des objectifs de performance qualitatives et quantitatives, des clauses relatives à la sous-traitance, des incidents liés aux TIC, les tests de pénétration, l’audit, les stratégies de sortie • Des fournisseurs alternatifs et des stratégies de sortie doivent être développés, documentés et testés régulièrement pour les services supportant les fonctions critiques ou importantes
Registre DORA	• Un registre des prestataires de services TIC doit être établi et 100 champs à renseigner parmi 10 tables de données • Ce registre nécessite la création (ou l’enrichissement) d’un LEI pour chaque prestataire et son parent ultime • Des informations sur les sous-traitants (jusqu’à deux niveaux de sous-traitants) doivent être collectées dans le registre
Organisation Groupe	• Les contrats des prestataires intra-groupe de service TIC doivent être revus pour les mettre aux normes applicables aux prestataires externes • Le registre DORA doit être géré au niveau consolidé et sous-consolidé

Parties prenantes concernées

De nombreuses équipes devront être **mobilisées** afin **de mettre en œuvre les exigences de DORA**

	Sécurité de l'information	Direction des Risques	Direction Informatique	Direction Achats	Direction Juridique	Direction générale
Cybersécurité	✓		✓			
Résilience opérationnelle		✓	✓			
Notification des incidents	✓	✓	✓			
Gouvernance et processus	✓	✓	✓	✓	✓	✓
Prestataires de services TIC			✓	✓	✓	
Registre DORA			✓	✓		

Toutes **les équipes métiers** devront également être sollicitées sur des sujets comme **l'inventaire des actifs informationnels** ou **l'identification des prestataires de services alternatifs.**

05

Objectifs & démarche

BEAM
& SAGALINK

ALETELA

Objectifs & démarche (1/2)

ALETELA BEAM & SAGALINK

Afin de se conformer aux exigences de la réglementation DORA, il est nécessaire de s'assurer de la mise en place du dispositif ci-dessous :

Référentiel organisationnel

Recenser, identifier et documenter de manière exhaustive toutes les fonctions « métiers », tous les rôles et toutes les responsabilités s'appuyant sur les TIC au sein de votre entité
Les fonctions « métier » identifiant notamment les « fonctions critiques ou importantes » au sens réglementaire (MiFID 2).

Inventaire des actifs informationnels

Recenser, identifier et documenter de manière exhaustive tous les actifs informationnels qui soutiennent les fonctions « métier »
Les actifs informationnels couvrent tout « ensemble d'informations, matérielles ou immatérielles, qui justifie une protection »

Inventaires des actifs de TIC

Recenser, identifier et documenter de manière exhaustive tous les actifs de TIC, en identifiant leur propriétaire et toutes les fonctions « métiers » qu'ils sont supportées
Les [illegible] sont [illegible] et [illegible] de vous [illegible] vous situés sur des sites

Inventaire des prestations TIC

Identifier et documenter tous les processus qui dépendent de prestataires tiers de services TIC, et les interconnexions avec des prestataires tiers de services TIC qui fournissent des services qui soutiennent des fonctions critiques ou importantes

CONTACTEZ-NOUS POUR LA VERSION COMPLÈTE DE CETTE ÉTUDE

Registre DORA

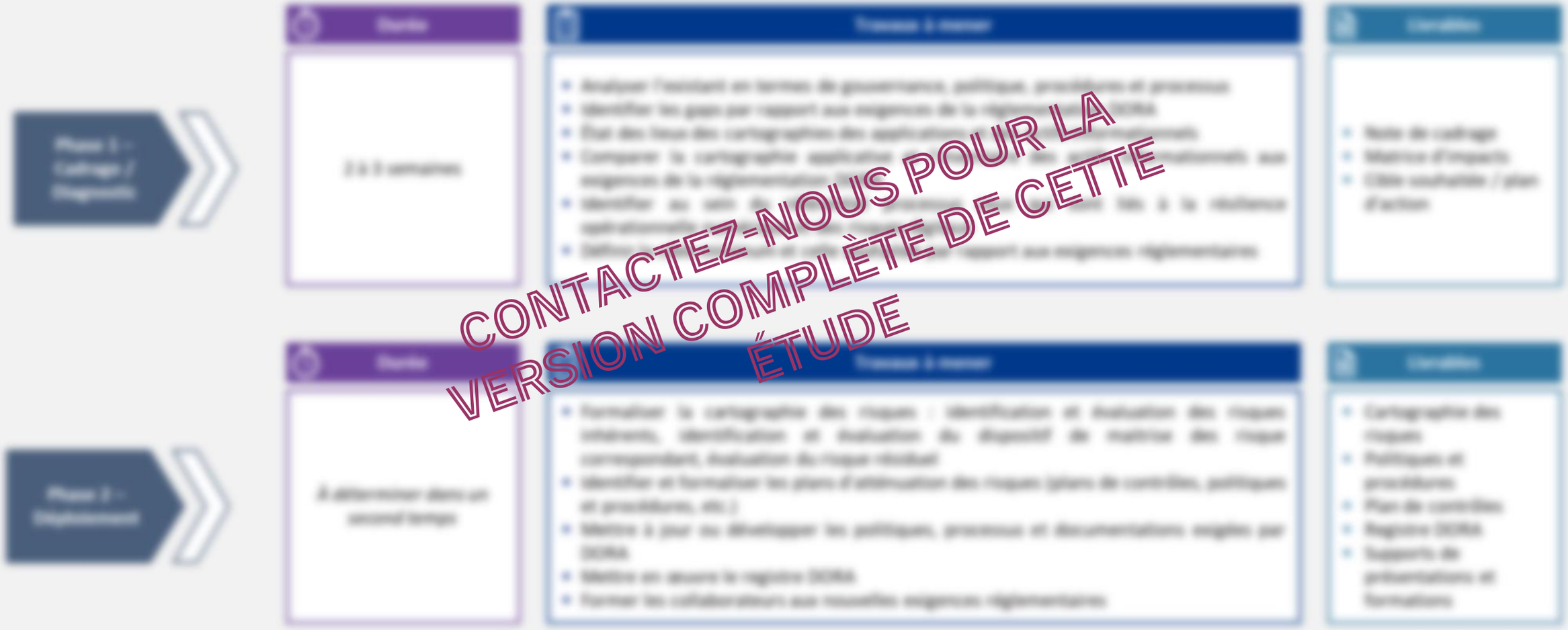
Recenser tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers de services TIC.
Le registre devrait détailler non seulement les informations contractuelles clés, mais également les services TIC rendus, les fonctions « métiers » supportées, des informations de « supply chain » listant jusqu'à deux niveaux de sous-traitants, les prestataires alternatifs identifiés, l'existence d'un plan de sortie, etc.

Production d'informations nécessaires pour alimenter le registre

Objectifs & démarche (2/2)

ALETELA BEAM & SAGALINK

Nous proposons la démarche suivante :



Nous contacter

BEAM&SAGALINK, cabinet de conseil en stratégie opérationnelle et en organisation, spécialisé dans les métiers de la gestion d'actifs, l'assurance, la banque privée, les services aux investisseurs, les marchés de capitaux et en transverse sur les fonctions finance et risques, l'ESG, la Data et le digital.
Le cabinet a été créé avec l'ambition de faire le lien entre les projets et les métiers de ses clients, en faisant preuve à la fois d'une maîtrise des techniques du conseil et d'une solide expertise dans les services financiers

ALETELA SAS est un cabinet de conseil indépendant spécialisé dans la réglementation des marchés et des services financiers dans l'UE et au Royaume-Uni. Le cabinet aide les sociétés de gestion d'actifs et autres entreprises financières à comprendre, analyser et mettre en œuvre les nouvelles réglementations.
ALETELA SAS a fait ses preuves en traduisant des textes réglementaires complexes en sujets compréhensibles par les parties prenantes, en évaluant les impacts commerciaux et en aidant à résoudre les problèmes techniques soulevés par les nouvelles réglementations

Mélanie IMBERT
Associée
Melanie.imbert@beamsagalink.com

Alain DUCASSE
Expert Réglementaire
Alain.ducasse@aletela.fr

Meryem EL HALFI
Consultante Senior Confirmée
Meryem.elhalfi@beamsagalink.com