PLAN D'ACTION

La BCE requiert un plan. Pouvez-vous le fournir ?

Face à l'essor de l'IA, les organisations doivent prouver leur préparation cyber. Décryptage des risques, des attentes réglementaires et des réponses possibles.

Ce qu'il faut retenir

La BCE exige des établissements dits « importants » un plan d'action cyber IA d'ici au 31 octobre 2026, adressé directement au directeur général. L'enjeu n'est pas de se conformer à de nouvelles règles, mais de démontrer concrètement l'application de DORA. À l'ère de l'IA, le temps entre vulnérabilité et attaque se compte désormais en minutes plutôt qu'en semaines, ce qui rend les processus de correction traditionnels inadaptés. La véritable question est donc : savez-vous précisément quels endpoints vous gérez, leur niveau de risque et votre capacité à intervenir en temps réel ?

01

Le contexte

Le 7 juillet 2026, la BCE a demandé aux directeurs généraux des banques placées sous sa supervision directe de remettre, d'ici au 31 octobre 2026, un plan d'action à leur équipe de surveillance conjointe (JST). Ce plan doit préciser les actions à engager, les responsables identifiés, les budgets et effectifs dédiés, ainsi qu'un calendrier d'exécution contraignant.

La BCE s'appuie sur DORA (règlement UE 2022/2554) sans créer de nouvelles obligations, mais en durcissant l'application des règles existantes. Cette démarche s'inscrit dans le prolongement de l'avertissement cyber publié par le Comité Européen du Risque Systémique (CERS) le 25 juin 2026, une première historique. Dans le même mouvement, la collecte annuelle des données sur les risques informatiques a été décalée à février 2027.

Implications pour les établissements français. La supervision de DORA relève de l'Autorité de contrôle prudentiel et de résolution (ACPR) pour les banques et les assureurs, et de l'Autorité des marchés financiers (AMF) pour les acteurs de marché. Avec la transposition de NIS2, l'ANSSI deviendra l'autorité nationale de référence et les obligations de cybersécurité concerneront environ 15 000 organisations supplémentaires. L'ACPR précise que ces évolutions n'ont aucun impact sur l'application immédiate de DORA.

02

Pourquoi le temps presse

Le véritable facteur d'accélération est l'IA utilisée par les attaquants. Ce qui exigeait autrefois des jours, voire des semaines de développement peut aujourd'hui être réalisé en quelques minutes, réduisant considérablement le temps disponible pour réagir.

Selon le CERS, les délais de réaction des défenseurs se réduisent fortement. Le standard historique des 90 jours avant divulgation perd ainsi une grande partie de son efficacité.

Les données illustrent l'accélération de la menace. Selon le CERS, le développement d'un exploit, qui nécessitait auparavant plusieurs jours ou semaines, peut désormais être réalisé en quelques minutes ou heures. Dans le même temps, le nombre de vulnérabilités recensées a augmenté de 49,5 % entre le premier semestre 2025 et le premier semestre 2026. Le CERT-EU rapporte également neuf incidents de sécurité ayant touché les institutions européennes en 2025, dont deux liés à des zero-days.

Les principaux enseignements de l'avertissement du CERS (ESRB/2026/3, 25 juin 2026) :

Les modèles d'IA les plus avancés ramènent le temps nécessaire au développement d'un exploit de plusieurs jours ou semaines à quelques minutes ou heures.

Le niveau de risque cyber systémique pour le secteur financier européen a été relevé d'« élevé » à « grave » en juin 2026.

À retenir : dans un contexte où le temps se compte désormais en heures plutôt qu'en semaines, l'avantage ne réside plus dans l'accumulation de contrôles, mais dans la capacité à voir, prioriser et démontrer sa posture de sécurité.

03

Ce que la BCE attend des établissements

Les 5 exigences de la BCE à satisfaire d'ici au 31 octobre 2026 :

1. Un plan d'action cyber IA transmis à la JST compétente.
2. Des actions concrètes, avec des échéances clairement définies.
3. Un responsable identifié pour chaque mesure.
4. Des moyens humains et financiers dédiés.
5. Des preuves tangibles de l'avancement des actions, disponibles à tout moment pour la JST.

La cyber-résilience : un enjeu de direction générale

Les autorités de supervision considèrent désormais la cyber-résilience comme une responsabilité de gouvernance.

La BCE place la responsabilité au niveau de la direction générale et attend une gouvernance claire, fondée sur des responsables identifiés, des moyens dédiés et un calendrier précis.

Le CERS qualifie le cyber de risque systémique, au même titre que d'autres risques de stabilité financière.

Les Five Eyes le présentent comme un risque d'affaires majeur relevant de la responsabilité de la direction.

En Europe, la BaFin considère également la cybersécurité comme un investissement stratégique et prioritaire.

L'Allianz Risk Barometer 2026 classe le cyber (42 %) et l'IA (32 %) parmi les principaux risques d'affaires mondiaux.

04

Ce que les autorités attendent des établissements

Malgré leurs rôles distincts, la BCE, le CERS, la BaFin, les Five Eyes, l'ENISA et le CERT-EU portent des messages convergents. Trois priorités se dégagent :

1. Assurer une visibilité en temps réel sur l'ensemble des actifs. La visibilité est le socle de la gestion des risques. La BaFin, la BCE et les Five Eyes exigent une vue complète du réseau et du système d'information pour prioriser les correctifs selon le risque. Sans visibilité fiable, les actions perdent en efficacité.

2. Accélérer la gestion des vulnérabilités et des correctifs. C'est l'exigence la plus récurrente des recommandations. La BaFin appelle à réduire les cycles de correction de plusieurs semaines à quelques jours selon le risque. La BCE en fait une priorité à court terme, tandis que le CERS souligne que l'exploitation peut désormais suivre la découverte d'une vulnérabilité en moins d'une journée. Mais accélérer sans visibilité ni contrôle accroît le risque opérationnel.

3. Réduire la surface d'attaque. Les Five Eyes recommandent de limiter les accès inutiles et l'exposition externe des systèmes. La BCE et l'ENISA ciblent aussi les actifs exposés à Internet, les logiciels tiers et les composants open source. Réduire efficacement la surface d'attaque suppose d'abord une visibilité complète de l'environnement.

Autres priorités récurrentes. Les autorités convergent aussi sur la gestion des systèmes obsolètes, la surveillance IA sous contrôle humain, les identités, les risques tiers et fournisseurs d'IA, les plans de réponse testés et une gouvernance portée par le conseil.

05

Les cinq questions de gouvernance à poser dès aujourd'hui

Les attentes de la BCE et du CERS se traduisent par cinq questions fondamentales auxquelles la direction générale, responsable du plan d'action, doit pouvoir répondre à tout moment.

1. Savons-nous précisément ce que nous exploitons ? Une visibilité en temps réel sur tous les actifs, y compris les systèmes inconnus ou obsolètes, est indispensable.

2. À quelle vitesse corrigeons-nous les vulnérabilités critiques ? La réponse doit s'appuyer sur des indicateurs mesurés et vérifiables.

3. Pouvons-nous démontrer nos progrès immédiatement ? Les preuves doivent être disponibles à tout moment, à partir d'une source de données fiable et unique.

4. Maîtrisons-nous réellement nos dépendances aux tiers ? Les accès, fournisseurs et dépendances critiques doivent être identifiés et documentés.

5. Qui en est responsable ? Chaque plan d'action exige un responsable clairement désigné, doté d'un mandat et de moyens adaptés.

Ces cinq questions portent moins sur l'existence de contrôles que sur la capacité à en démontrer l'efficacité, la rapidité et la gouvernance.

06

De l’exigence réglementaire à l’exécution opérationnelle

Dans un contexte où l’IA accélère le passage de la vulnérabilité à l’exploitation, un plan d’action crédible doit reposer sur trois capacités : voir l’exposition réelle, prioriser les risques critiques et agir rapidement avec des preuves vérifiables.

Avec **Tanium Atlas**, ces capacités sont réunies dans une approche unifiée et gouvernée. La plateforme connecte les données issues des endpoints, des vulnérabilités, de l’exposition externe, du cloud et des identités afin d’aider les équipes IT et sécurité à comprendre où se situe le risque réel et quelles actions doivent être engagées en priorité.

Autonomous Exposure Management identifie les expositions et chemins d’attaque les plus critiques, notamment lorsqu’ils relient des actifs exposés à Internet, des endpoints vulnérables et des ressources sensibles. L’objectif est de réduire la surface d’attaque en fonction de l’impact réel sur le risque, plutôt que de scores isolés.

Autonomous Patch Management traduit cette priorisation en action : les correctifs sont orchestrés à grande échelle, suivis en temps réel et documentés. Les équipes peuvent ainsi prouver la rapidité de remédiation, les décisions prises et les progrès accomplis.

Les capacités **Security Operations** de Tanium renforcent cette approche en accélérant l’investigation, la chasse aux menaces et les workflows de réponse, tout en garantissant contrôle et traçabilité. Pour la direction générale, l’enjeu est clair : voir, décider, agir et prouver en continu.

Sources

- BCE, supervision bancaire, courrier aux directeurs généraux des établissements importants (réf. SSM-2026-0301), 7 juillet 2026. bankingsupervision.europa.eu
- CERS, avertissement ESRB/2026/3 « on systemic cyber risks stemming from frontier artificial intelligence models », 25 juin 2026. esrb.europa.eu
- ENISA, Threat Landscape 2025, publié en octobre 2025 (période juillet 2024 à juin 2025). enisa.europa.eu
- FIRST, 2026 Mid-Year Vulnerability Forecast, 15 juin 2026 (35 364 nouvelles vulnérabilités au premier semestre 2026, contre 23 656 un an plus tôt). first.org
- CERT-EU, Threat Landscape Report 2025 : A Year in Review, publié en avril 2026. cert.europa.eu
- DORA, règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier, 14 décembre 2022.
- BCE, Supervisory Banking Statistics T1 2026 (nombre d’établissements importants), 19 juin 2026. bankingsupervision.europa.eu
- ACPR, FAQ DORA (application de DORA indépendamment du calendrier de transposition de NIS2). acpr.banque-france.fr
- BaFin, prises de position publiques sur la cybersécurité : le président Mark Branson et le directeur exécutif Nikolas Speer (discours, juin 2026). bafin.de
- Five Eyes, lignes directrices communes sur les cybermenaces accélérées par l’IA (cinq mesures prioritaires), 2026.
- Allianz, Risk Barometer 2026 (enquête auprès de 3 338 experts en gestion des risques). allianz.com

Tanium n’entretient aucun lien avec la BCE, le CERS, l’ACPR, la BaFin ni aucune autre autorité de supervision citée, et ne revendique aucun soutien de leur part. Toutes les affirmations relatives aux sujets réglementaires sont citées avec leurs sources d’origine.