AFG

LePointsur

Cybersécurité :

SGP, comment anticiper les risques ?

Faire face aux nouvelles exigences Cybersécurité et Résilience

Jeudi 11 décembre 2025
9h30-11h00

AVERTISSEMENT

L’intervention des intervenants est proposée à titre d’information ou d’exemple pour présenter aux participants une pratique du marché applicable, une innovation en matière de technologie ou d’organisation. Cette présentation n’est pas une incitation pour les participants à utiliser les services des intervenants ou des sociétés pour lesquels ils travaillent, ni une offre commerciale.

L’AFG ne garantit pas la conformité règlementaire de cette proposition.

Aussi il appartient à chaque participant :

- de vérifier cette conformité au regard de sa situation propre
- de s’assurer que les propositions présentées sont adaptées à sa situation en vérifiant notamment si sur le marché d’autres offres sont plus pertinentes au regard de sa situation.

Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

Introduction

Laure Delahousse
Directrice générale de l'AFG

« Point Sur »
Cybersécurité :

SGP, comment anticiper les risques ?

1. AMF : premiers retours DORA
2. KPMG : Les tendances cyber et résilience
3. GT Cyber : Fiche Cyber IA

Cybersécurité : SGP, comment anticiper les risques ?

Orateurs

Valentine Bonnet
Directrice Gouvernement d'entreprise et Conformité, en charge du GT cybersécurité de l'AFG

Bruno Buresi
Adjoint à la Directrice des contrôles des SGP et des CIF de l'AMF

Walif El Hitti
CISO, Comgest

Frédéric Gleizer
RSSI, BNP Paribas Asset Management

Wilfried Lauber
Président du GT Cybersécurité de l'AFG et RSSI adjoint d'Amundi

Vincent Maret
Associé, Responsable du pôle Cybersécurité et Protection des données personnelles & AI Trust Lead, KPMG France

Olivier Pallany
Group CISO & DPO, Sienna Investment Managers

AFG

LePointsur

Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

N’hésitez pas à poser vos questions aux orateurs sur la plateforme

Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

AMF : premiers retours DORA

Bruno Buresi
Adjoint à la Directrice des contrôles des SGP et des CIF de l'AMF

Wilfried Lauber
Président du GT Cybersécurité de l'AFG et RSSI adjoint d'Amundi

A NOTER

LISTE DES CTTP

- **Accenture plc**
- **Amazon web Services EMEA Sarl**
- **Bloomberg L.P.**
- **Capgemini SE**
- **Colt Technology Services**
- **Deutsche Telekom AG**
- **Equinix (EMEA) B.V.**
- **Fidelity National Information Services, Inc.**
- **Google Cloud EMEA Limited**
- **International Business Machine Corporation**
- **InterXion HeadQuarters B.V.**
- **Kyndryl Inc.**
- **LSEG Data and Risk Limited**
- **Microsoft Ireland Operations Limited**
- **NTT DATA Inc.**
- **Oracle Nederland B.V.**
- **Orange SA**
- **SAP SE**
- **Tata Consultancy Services Limited**

Les sociétés de gestion se trouvant régies par le règlement DORA, qui intègre des obligations concernant la sous-traitance de services ou de fonctions à des prestataires, **les Orientations de l'ESMA sur la sous-traitance à des prestataires cloud** ont été modifiées et **excluent désormais les SGP** (ces orientations, dont le périmètre a été modifié, ne s'appliquent désormais qu'à certains dépositaires de FIA et d'OPCVM qui ne seraient pas déjà couverts par DORA).

Cybersécurité : SGP, comment anticiper les risques ?

AMF : premiers retours DORA

Questions des membres AFG

Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

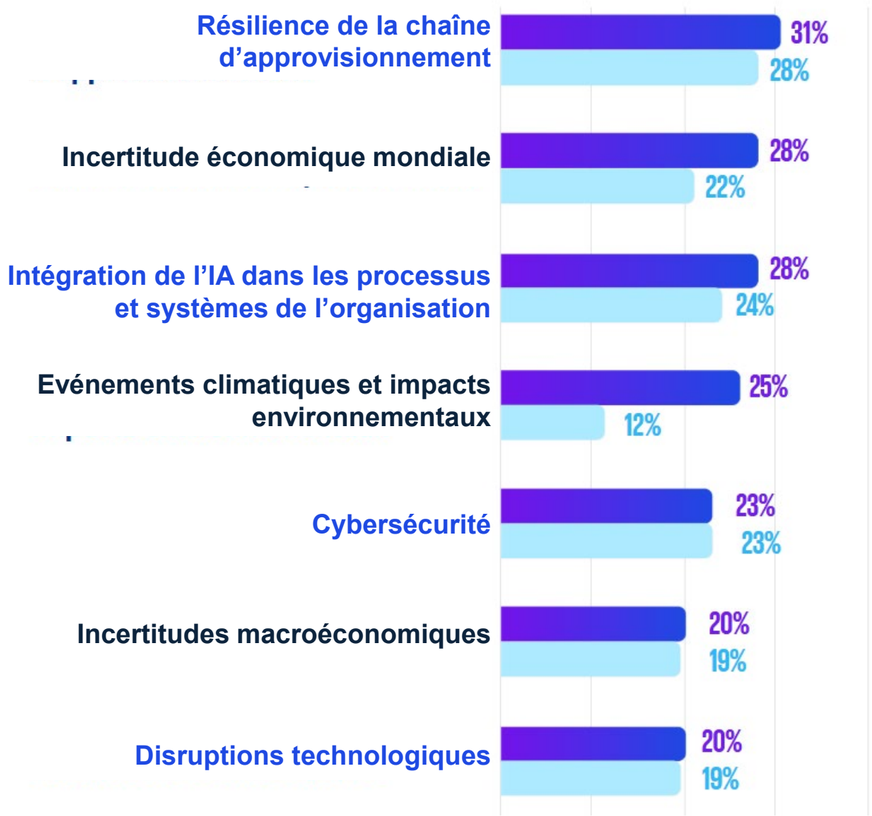
KPMG : Les tendances cyber et résilience

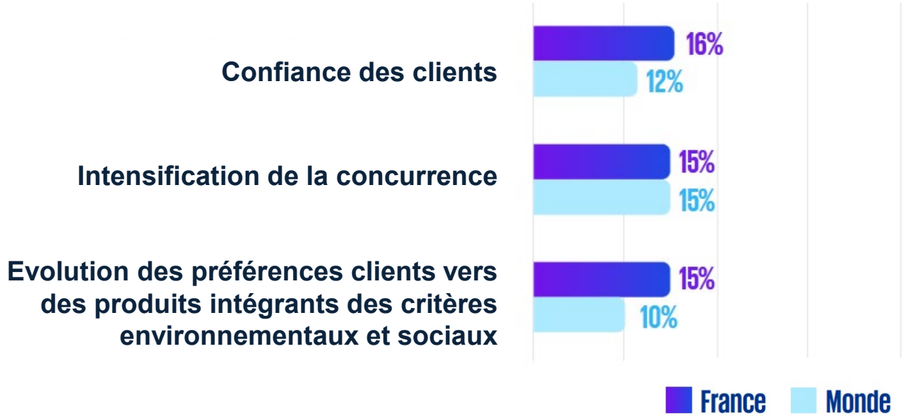
Valentine Bonnet
Directrice Gouvernement d'entreprise et Conformité, en charge du GT cybersécurité de l'AFG

Vincent Maret
Associé, Responsable du pôle Cybersécurité et Protection des données personnelles & AI Trust Lead, KPMG France

La cybersécurité et la résilience, un risque majeur pour les dirigeants

Top 10 des pressions et défis influençant le plus les décisions des dirigeants à court terme





La révolution de l'IA engendre des risques nouveaux, variés et parfois inattendus.

Risques liés à l'impact de l'IA

Sur-confiance, impact sur l'emploi, désinformation, érosion de la vie privée, impact sur les relations sociales, etc.

Risques liés aux caractéristiques intrinsèques de l'IA

Biais, raccourcis, contenus hors distribution, hallucination, reward hacking, contenu toxique, manque d'explicabilité, mémorisation, capacités de raisonnement limitées, fragilité, atteinte à la privacy

Risques liés aux attaques malveillantes sur l'IA

Empoisonnement de données, porte dérobée, contenu adversarial, extraction de données, extraction de modèles, prompt injection, jailbreak

Risques liés à l'utilisation malveillante de l'IA

Deepfake, phishing, codage de logiciels malveillants, automatisation de cyberattaques, etc.

Des pirates chinois ont mené des cyberattaques en un clic grâce à l'IA d'Anthropic

Novembre 2025

S'adapter aux menaces liées à l'IA.

- Montée en compétences de l'équipe CISO sur l'IA
- Collaboration avec les praticiens de l'IA
- Adaptation des politiques, univers des risques
- Suivi des incidents liés à l'IA, des articles académiques, etc.
- Sécurisation des infrastructures de l'IA
- Expérimentation d'outils et techniques (ex : red teaming IA, pare-feu IA)
- Mise à jour des processus de réponse aux incidents et de gestion des crises

Et demain, l'IA agentique…

POC*: proof of concept

L’IA Act : une réglementation de l'UE visant à réduire les risques générés par l'utilisation de l’IA

Plusieurs types d'acteurs sont concernés par l’IA ACT

- Les fournisseurs, qui développent des systèmes d’IA
- Les déployeurs, qui utilisent les systèmes d'IA

Amendes pouvant atteindre 7 % du chiffre d'affaires mondial

L'IA Act concernera toutes les organisations, à l'intérieur et à l'extérieur de l’UE

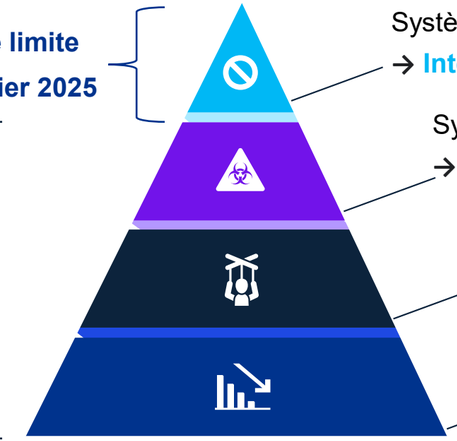
- Fournisseurs et déployeurs dans l'UE
- En dehors de l'UE si les systèmes d'IA sont utilisés dans l'UE

Il y aura plusieurs régulateurs au niveau au niveau national

Publication d’un projet de loi en septembre 2025, désignant notamment la CNIL et l’ACPR comme régulateurs en fonction des cas d’usage.

Date limite
2 février 2025

Date limite
2 août 2026
ou Décembre 2027*



Systèmes d'IA générant des risques inacceptables
→ **Interdit**

Systèmes d'IA générant des risques élevés
→ **Doit se conformer à de nombreuses exigences**

Systèmes d'IA générant des risques limités (interaction avec les personnes, génération de contenu)
→ **Doit se conformer à certaines exigences**

Autres systèmes d’IA
→ **Aucune exigence**

***La Commission Européenne a proposé son “paquet omnibus” le 19 novembre 2025: un ensemble d’amendements pour « simplifier » le cadre numérique européen, couvrant notamment l’IA Act et son application.**

Des gestionnaires d'actifs moins impactés que la banque de détail, le crédit à la consommation et l'assurance.

Le CISO en tant que partie prenante clé pour la conformité à l’IA Act.

- Collaboration
- Inventaire des systèmes d'IA
- Pare-feu IA, red teaming IA

Assurer la résilience implique de prendre en compte des scénarios plus larges que de simples cyberattaques

De nombreux sites internet paralysés par une panne chez le fournisseur Cloudflare

Novembre et décembre 2025

Cyberattaques : les usines de Jaguar Land Rover au Royaume-Uni et les usines de Asahi au Japon à l'arrêt

Octobre 2025

Microsoft Azure, deuxième plateforme cloud au monde, touché par une panne

Octobre 2025

Harvest : fuite de données et paralysie du secteur de la gestion de patrimoine

Mars 2025

Une panne mondiale touche AWS : Internet et des dizaines de services paralysés

Octobre 2025

Les univers de risques, les plans de reprise après sinistre et de continuité d'activité, les processus de gestion de crise et les exercices doivent être continuellement mis à jour pour prendre en compte de nouveaux scénarios

Les questions géopolitiques ont un impact accru sur le cyberespace

Nombre croissant de réglementations et d'exigences liées aux risques cyber et technologiques à travers le monde

RGPD, AI act, DORA, MICA, NIS2 eIDAS, ePrivacy, CRA, CCPA/CPRA, lois étatiques américaines sur la vie privée, IoT et IA, CSL, PIPL, SWIFT CSP, PCI-DSS, etc.

Réglementations imposant l'hébergement local des données (Chine, Turquie)

Tesla ouvre un datacenter en Chine pour conserver ses données au niveau local, conformément à la réglementation chinoise

Mai 2021

Impact des conflits sur les services technologiques

Microsoft coupe les mails de la Cour Pénale Internationale face aux aléas géopolitiques

Mai 2025

Suivre les projets de réglementations et les réglementations adoptées dans le monde entier

Préparer des plans d'urgence en cas de conflit régional, par exemple en coupant les réseaux

Être impliqué dans les projets de cloud souverain

Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

KPMG : Les tendances cyber et résilience

Questions des membres AFG

Cybersécurité : SGP, comment anticiper les risques ?

AFG

GT Cyber : Fiche Cyber « Intelligence Artificielle »

LePointsur

Wilfried Lauber
Président du GT Cybersécurité de l'AFG et RSSI adjoint d'Amundi

Walif El Hitti
CISO, Comgest

Olivier Pallany
Group CISO & DPO, Sienna Investment Managers

Frédéric Gleizer
RSSI, BNP Paribas Asset Management

Bénéfices et risques stratégiques de l’IA pour les SGP


AFG

FICHE PRATIQUE

CYBERSECURITE DE L'INTELLIGENCE ARTIFICIELLE :
LEVIER STRATEGIQUE POUR LES SOCIETES DE GESTION

L'IA, un risque à maîtriser face à un impératif stratégique

L'Intelligence Artificielle (IA) offre des opportunités de croissance et d'optimisation majeures pour votre société de gestion, notamment par l'automatisation, l'analyse avancée et l'aide à la décision tout en introduisant des risques significatifs.

Au-delà des problématiques posées en termes de gouvernance et d'éthique (opacité des décisions, absence de supervision), l'IA amplifie les risques existants et en introduit de nouveaux, liés notamment au caractère extrêmement accessible généré par l'utilisation du langage naturel.

Notre approche vise à transformer ces défis de sécurité pour les SGP en **avantages compétitifs** en structurant votre sécurité autour de 5 piliers fondamentaux :

1. **Maîtrise des vulnérabilités spécifiques à l'IA**
2. **Intégration du facteur humain**
3. **Stratégie de gestion des risques cyber liés à l'IA : Définir votre posture**
4. **Gouvernance des risques & Shadow AI**
5. **Protection de la Donnée : Sécuriser l'actif critique**

1. Maîtrise des vulnérabilités spécifiques à l'IA

Les systèmes d'IA ouvrant à des vulnérabilités, il est essentiel de maîtriser les vecteurs d'attaque spécifiques liés à l'IA. Pour ce faire, **comprendre les techniques d'exploitation est la première étape pour bâtir une défense robuste**.

ALTERATION / INJECTION DE REQUÊTE
Prompt injection

MECANISME :
- L'attaquant insère des instructions cachées (ex : texte invisible dans un document Word) pour manipuler la réponse de l'IA

RISQUE POUR LA SGP :
- Fuite d'informations sensibles ou exécution d'actions contraires aux règles de sécurité

EMPOISONNEMENT DES DONNEES
Data poisoning

MECANISME :
- Introduction de données malveillantes dans les jeux d'entrainement. (Ex : Faux emails "propres" pour tromper un modèle de détection de spam)

RISQUE POUR LA SGP :
- Perte de fiabilité et d'intégrité des modèles IA, qui apprennent de mauvais comportements

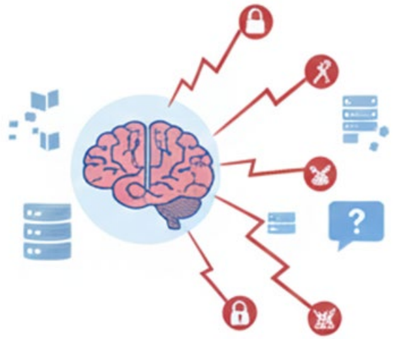
CONTOURNEMENT DE FILTRES
Jailbreaking

MECANISME :
- Utilisation de ruse linguistique et de commandes détournées pour outrepasser les garde-fous des modèles

RISQUE POUR LA SGP :
- Obtention d'informations confidentielles ou génération de contenu interdit

Nouvelle fiche Cyber IA

VULNÉRABILITÉS SPÉCIFIQUES À L'IA ET VECTEURS D'ATTAQUE



Risques liés à l'IA

L'intelligence artificielle amplifie les risques existants et en crée de nouveaux,
notamment à cause du langage naturel accessible.

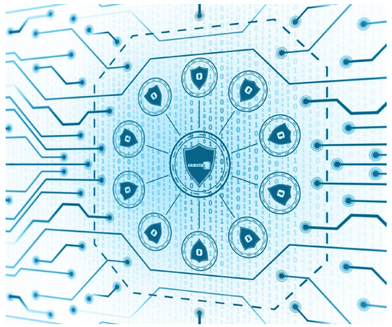
Enjeux de gouvernance

L'IA soulève des défis de gouvernance comme l'opacité des décisions et l'absence de supervision efficace.

Approche sécuritaire

Structurer la sécurité autour de cinq piliers fondamentaux pour transformer les vulnérabilités en avantages compétitifs.

Principaux vecteurs d'attaque et risques associés



VECTEUR D'ATTAQUE	MÉCANISME	RISQUE POUR LA SGP
Altération/Injection de Requête (Prompt Injection)	L'attaquant insère des instructions cachées (ex: texte invisible dans un document Word) pour manipuler la réponse de l'IA.	Fuite d'informations sensibles ou exécution d'actions contraires aux règles de sécurité.
Empoisonnement des Données (Data Poisoning)	Introduction de données malveillantes dans les jeux d'entraînement. (Ex : Faux emails "propres" pour tromper un modèle de détection de spam).	Perte de fiabilité et d'intégrité des modèles IA, qui apprennent de mauvais comportements.
Contournement des Filtres (Jailbreaking)	Utilisation de ruse linguistique et de commandes détournées pour outrepasser les garde-fous des modèles.	Obtention d'informations confidentielles ou génération de contenu interdit.

Toute évolution technologique crée des opportunités… mais aussi des risques. Les connaître, c'est mieux les anticiper et mieux les gérer.

LE FACTEUR HUMAIN : LA SENSIBILISATION, UN ÉLÉMENT CLÉ …

Sensibilisation

- **Connaitre le fonctionnement de l'IA, ses limites, ses risques**
- **Former, un impératif pour les SGP**
- **Définir les bonnes pratiques et les bonnes postures**

Accompagner les salariés de la SGP avec des bonnes pratiques, comme la vérification des sources et le signalement d'anomalies, est un pilier de la sécurité.

Mise en place d'une charte d'usage de l'IA

- **Encadrement de l'usage de l'IA**
- **Engagement cybersécurité et confidentialité**
- **Contrôles et sanctions**
- **Socle de confiance collaborateur**

Ce cadre clair et sécurisé établit une base de confiance pour tous les collaborateurs dans l'usage de l'IA.

La gestion des risques liés à l'IA, comme en cybersécurité, repose avant tout sur le facteur humain

Pour votre SGP, adopter une stratégie adaptée à ses risques

Stratégie restrictive	Stratégie ouverte
Blocage systématique	Blocage ciblé
Sécurité et conformité maximales	Agilité et productivité accrues
Risque de limiter l'innovation	**Exige une forte culture sécurité**

Déploiement en interne uniquement pour les cas sensibles ou stratégiques.

Ouverture progressive avec filtrage des usages.

Ouverture large avec sensibilisation et formation continue.

- **Cadre** : définition et justification claires des outils IA autorisés et interdits.
- **Sélection rigoureuse** : évaluation basée sur Sécurité, Conformité et Fiabilité des outils/fournisseurs.
- **Mise à jour** : révision régulière minimum des autorisations/interdictions selon les évolutions de la technologie et des menaces.
- **Communication transparente** : information claire et accessible des utilisateurs.
- **Gouvernance collaborative** : implication IT, sécurité, juridique/conformité et métiers.
- **Surveillance continue :** collecte de feedbacks et ajustements rapides basés sur les usages et incident.

Tout commence par une gouvernance claire et efficace pour votre SGP

Le **Shadow AI**, qui correspond à l'utilisation de l'IA par des collaborateurs de la SGP de façon non autorisée, peut être **le reflet d'un besoin interne non couvert**.

Structurer l'organisation

Mettre en place une **gouvernance collaborative** intégrant les personnes en charge de la **cybersécurité, conformité, risques, données personnelles, IT, juridique, et Direction Générale**, pour établir :

- Rôles et responsabilités
- Suivi des usages
- Sécurité dans les projets IA

Cartographier les usages de l'IA

Inventorier les usages est un prérequis!

→ Identifier les risques

→ Mis en place de mesures adaptées

Prendre des mesures préventives essentielles

- ✓ Cohérence des prompts
- ✓ Intégrité et qualité des données
- ✓ Détection d'anomalies
- ✓ Alertes par l'utilisateur

PROTECTION DES ACTIFS CRITIQUES DE LA SGP

Sécuriser les environnements/accès

- Environnements contrôlés/sécurisés
- Classification des données
- Contrôle d'accès/gestion des habilitations

Protéger contre la fuite d'information

- Vecteurs de fuites identifiés
- Données d'entraînement/d'inférence protégées
- Contrôle de prompts
- Surveillance/journalisation

Maîtriser la relation fournisseur

- Propriété intellectuelle
- Maîtrise des traces
- Protection des actifs critiques et algorithmes propriétaires

La sécurité des données est la garantie de la confiance et de la conformité pour votre SGP

Cybersécurité : SGP, comment anticiper les risques ?

AFG

Fiche AFG Cyber « Intelligence Artificielle »

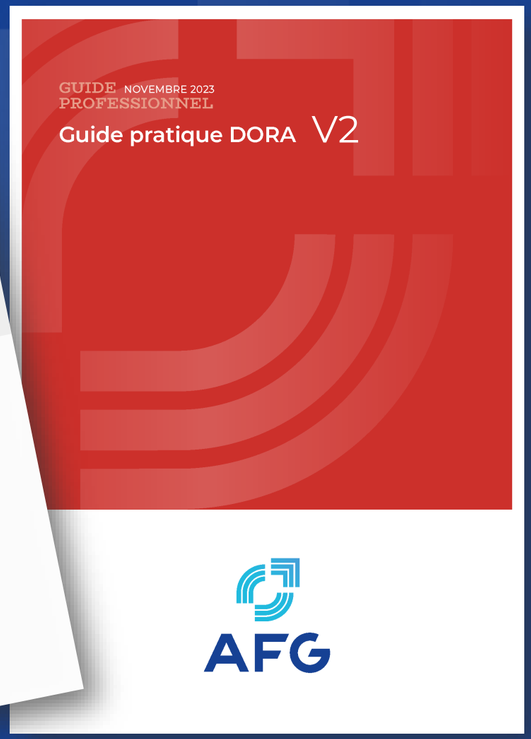
LePointsur

Questions / Réponses des membres AFG

Publications du GT cybersécurité AFG

disponibles sur le site AFG

PUBLICATIONS 2025



Cybersécurité : SGP, comment anticiper les risques ?

AFG

LePointsur

Rappel :

La vidéo de cette conférence, les slides et les documents cités seront disponibles prochainement sur le site de l’AFG

Ensemble, s’investir pour demain

Merci !

AFG

17 Square Edouard VII · 75009 Paris · +33 (0)1 44 94 94 00 ■ Avenue des Arts 56 ■ www.afg.asso.fr