∞drive

Gouvernance digitale : protégez vos décisions les plus stratégiques

Sommaire

Introduction : la gouvernance sous pression

Ransomwares, fuites d'informations sensibles, hameçonnage ciblé : en 2024, 91 % des grandes entreprises françaises ont subi une cyberattaque (source : CESIN, 2025). Les réunions stratégiques – conseils d'administration, comités exécutifs, comités d'investissement – concentrent des informations parmi les plus convoitées par les cybercriminels : projets de fusion-acquisition, rémunérations, cessions d'actifs, contrats confidentiels, litiges en cours.

Pourtant, nombre de ces instances continuent de fonctionner avec des pratiques héritées d'un monde pré-numérique : documents envoyés par email non chiffré, stockage sur des drives personnels ou non européens, impression papier sans destruction sécurisée. Dans un contexte où les attaques sont de plus en plus ciblées et sophistiquées, ces usages ouvrent la voie aux intrusions et exposent directement les dirigeants à des risques juridiques et réputationnels.

Parallèlement, la montée en puissance du cadre réglementaire – avec les directives européennes NIS2 et le règlement DORA – accentue la pression sur les organes de gouvernance. Ces textes imposent aux entreprises une gouvernance numérique robuste, traçable et souveraine. Désormais, il ne suffit plus de protéger l'information : il faut être capable de prouver la protection et la résilience en cas d'audit ou d'incident.

Ce guide vous propose un état des lieux actualisé des menaces et des obligations, une méthode structurée pour bâtir une gouvernance numérique résiliente, et des retours d'expérience concrets pour déployer des solutions souveraines comme Oodrive Meet.

Bonne lecture !

1 ↘

NIS2 et DORA : un tournant réglementaire majeur

Deux textes structurent désormais les obligations des conseils d'administration et des comités exécutifs : **la directive NIS2** et **le règlement DORA**.

La directive NIS2

Transposée en droit français depuis octobre 2024, NIS2 s'applique à un large spectre d'organisations jugées critiques ou importantes. Elle impose :

- Une responsabilisation accrue des dirigeants en matière de cybersécurité ;
- Une évaluation continue des risques sur les systèmes critiques ;
- Des mesures de gestion des accès, de journalisation et de traçabilité des actions ;
- La notification d'incidents de sécurité dans un délai de 24 à 72 heures.

L'un des changements majeurs : les **conseils d'administration sont désormais directement impliqués dans la stratégie de cybersécurité**. En cas de manquement, leur responsabilité personnelle peut être engagée.

Le règlement DORA

Applicable dès janvier 2025 pour les secteurs financiers et assurantiels, DORA (Digital Operational Resilience Act) va encore plus loin :

- Les entreprises doivent démontrer leur **continuité opérationnelle** pour toutes leurs fonctions critiques ;
- Elles doivent **maîtriser leur chaîne de sous-traitance** numérique ;
- Elles sont tenues de réaliser des tests réguliers de résilience et de réaction à incident.

Ces deux textes convergent : ils exigent des organes de gouvernance qu'ils **mettent en place un cadre de gestion sécurisée et documentée** des réunions stratégiques. L'absence de preuve ou de traçabilité devient une faille majeure, tant sur le plan juridique que réputationnel.

2 ↘

Chiffres clés et cybermenaces sur les conseils d'administration

68%

des violations de données impliquent des erreurs humaines, souvent dans le cadre d'échanges non sécurisés de documents sensibles

→ *(source : IBM Cost of a Data Breach Report, 2024).*

91%

des grandes entreprises françaises ont subi une cyberattaque en 2024

→ *(source : CESIN, 2025).*

3,59 M€

le coût moyen d'une violation de données en France

→ *(source: IBM Cost of a Data Breach Report, 2025)*

Parmi les pratiques à risque encore trop fréquentes

- Envoi de convocations et documents confidentiels par email non chiffré
- Stockage de dossiers de conseil sur des drives personnels ou des solutions non souveraines
- Absence de traçabilité des accès aux documents partagés
- Impression papier de documents sensibles, sans destruction sécurisée

Des attaques de plus en plus ciblées

Les cybercriminels ont affiné leurs techniques : **Business Email Compromise**, **spear phishing**, injection de logiciels malveillants lors de visioconférences… Les décideurs eux-mêmes sont désormais en première ligne. Chaque réunion stratégique devient une cible potentielle.

Business Email Compromise (BEC)

Fraude ciblée où des cybercriminels usurpent ou compromettent une adresse email professionnelle afin de tromper une entreprise et détourner des fonds ou des informations sensibles.

Spear Phishing

Attaque de phishing hautement ciblée, où un cybercriminel envoie un message personnalisé à une personne ou une organisation spécifique pour voler des informations sensibles ou installer un malware.

3 ↘

Méthodologie d’une gouvernance digitale sécurisée

Gestion du projet et conduite du changement

Face à ces défis, la dématérialisation sécurisée des réunions stratégiques n'est plus une option mais un impératif. Elle répond à **trois enjeux majeurs** :

Réduire les risques de fuite et d'erreur humaine grâce à des espaces sécurisés et des accès maîtrisés.

Simplifier la préparation et la tenue des réunions avec des processus unifiés et des documents centralisés.

Garantir la conformité réglementaire aux exigences NIS2, DORA et RGPD.

Méthodologie en 6 étapes

1. **Cartographier les instances et documents critiques** (conseils, comités d'investissement, convocations, PV, contrats stratégiques).
2. **Évaluer les pratiques actuelles** et identifier les failles (emails non chiffrés, stockage non souverain, accès non contrôlés).
3. **Définir les rôles et responsabilités** (Secrétaire Général, CA, DSI, RSSI).
4. **Choisir une solution souveraine** (qualifiée SecNumCloud, certifiée eIDAS, ISO 27001).
5. **Formaliser les procédures internes :** gestion des accès, conservation et destruction des documents.
6. **Former et sensibiliser les administrateurs** aux bons réflexes cyber (sessions dédiées, fiches pratiques).

Clés de réussite

- Impliquer le Secrétariat Général et la DSI dès la phase de cadrage.
- Créer un comité de pilotage interfonctionnel.
- Prioriser la simplicité d'usage pour les administrateurs (critique pour l'adoption).
- Capitaliser sur les retours d'expérience internes et externes pour affiner le dispositif.

Bonnes pratiques à adopter

La réussite d'une gouvernance numérique passe par des pratiques rigoureuses, partagées entre toutes les parties prenantes. Voici les meilleures pratiques observées chez nos clients.

Efficacité opérationnelle

- Utilisez des plateformes qualifiées (SecNumCloud, ISO 27001, eIDAS) pour héberger vos données.
- Évitez les partages par email ou solutions grand public non européennes.

Mettre en place une politique de gestion des accès rigoureuse

- Attribuez des droits différenciés selon les profils : lecture seule, modification, téléchargement interdit, etc.
- Adoptez le principe du moindre privilège : n'accorder que les accès strictement nécessaires à chaque utilisateur.

Former les utilisateurs aux risques et aux bons réflexes

- Planifiez des sessions de sensibilisation ciblées pour les membres du conseil. Intégrez des scénarios concrets (perte de document, canal non sécurisé, usurpation).

Intégrer la sécurité dès la planification des réunions

- De l'ordre du jour à la signature du compte-rendu, chaque étape doit être pensée dans un cadre sécurisé et traçable. Utilisez une solution conforme à la politique de sécurité de votre entreprise.

Vérifier la conformité réglementaire des outils utilisés

- Tous les outils numériques employés dans les instances stratégiques doivent être audités régulièrement : conformité RGPD, hébergement UE, compatibilité eIDAS, journalisation.

Créer un plan de réponse en cas d'incident

- Formalisez un plan d'action en cas de compromission de documents, de perte d'accès ou d'attaque ciblée. Ce plan doit inclure les responsabilités, les délais de notification et les modalités de reprise.

Intégrer les obligations NIS 2 et DORA dans la gouvernance documentaire

- Ajoutez aux processus internes des clauses précisant les responsabilités cyber, les obligations de continuité, les délais de réaction et d'auditabilité.

4 ↘

Choisir la bonne solution de gouvernance : critères et application

Dans un contexte où les conseils d'administration et comités stratégiques traitent des informations sensibles, le choix d'une solution de gouvernance numérique n'est pas qu'une question d'ergonomie. C'est une décision qui engage la sécurité de l'entreprise, sa conformité réglementaire, et la fluidité de ses processus décisionnels.

Checklist : Les 8 critères clés pour bien choisir votre solution

Utilisez cette liste comme base d'évaluation de toute solution de gouvernance numérique, que ce soit dans le cadre d'un appel d'offres, d'un renouvellement ou d'un audit interne.

	Oui	Non
Sécurité & Souveraineté		
Les données sont-elles hébergées 100 % en Europe ?	●	●
La solution est-elle qualifiée SecNumCloud /ISO 27001 ?	●	●
Les échanges sont-ils chiffrés de bout en bout ?	●	●
Conformité		
La solution est-elle alignée avec RGPD, NIS2, DORA ?	●	●
Existe-t-il une journalisation complète des accès et actions ?	●	●
Gestion des accès		
Peut-on mettre en place une MFA ?	●	●
Les rôles sont-ils différenciés (membre, invité, observateur) ?	●	●
Les accès peuvent-ils être restreints par document ?	●	●
Cycle complet de réunion		
L'ordre du jour, les documents et PV sont-ils centralisés ?	●	●
La signature électronique est-elle intégrée ?	●	●
La gestion des versions est-elle transparente ?	●	●
Traçabilité		
Chaque action est-elle tracée ?	●	●
Les logs sont-ils exportables facilement ?	●	●
Expérience utilisateur		
L'interface est-elle intuitive ?	●	●
L'accès mobile et hors ligne est-il disponible ?	●	●
Des formations rapides sont-elles prévues ?	●	●
Interopérabilité		
L'outil s'intègre-t-il avec SSO, calendriers, messagerie ?	●	●
Une API est-elle disponible ?	●	●
Accompagnement		
Un support francophone avec SLA est-il prévu ?	●	●
Y a-t-il des formations adaptées aux profils ?	●	●

Oodrive Meet au service des conseils d'administration

Solution de gestion des réunions de gouvernance souveraine, conçue pour les conseils d'administration, COMEX ou autres instances considérées comme sensibles, **Oodrive Meet** centralise **tous les éléments critiques** des réunions stratégiques – convocations, ordres du jour, documents préparatoires, comptes rendus – dans un environnement hautement sécurisé.

Les principaux bénéfices

Maîtrise complète du cycle de réunion

- Planification, préparation, conduite et suivi intégrés dans un portail unique
- Convocations et relances automatisées
- Centralisation documentaire et génération d'un boardbook accessible en contenu

Collaboration fluide et expérience moderne

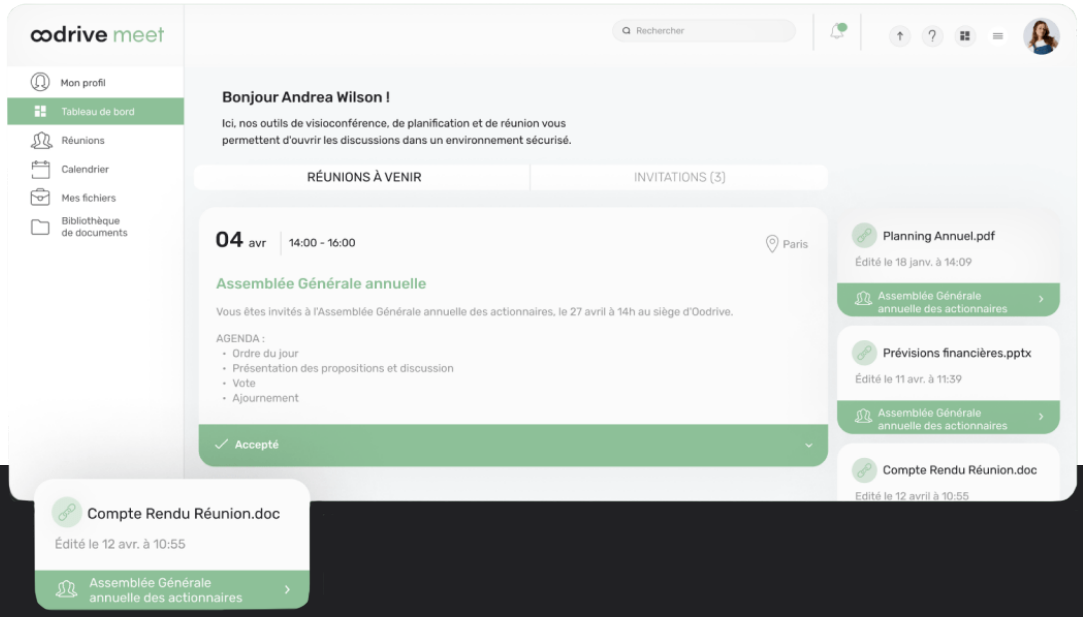
- Interface unifiée web & mobile, accessible même hors ligne.
- Visioconférence intégrée (MS Teams, Tixeo)
- Outils intéractifs : votes, annotations collaboratives, signature électronique

Sécurité et souveraineté de bout en bout

- Hébergement en France (SecNumCloud), sans lois extraterritoriales
- Chiffrement HSM, supervision et journalisation
- Gestion granulaire des droits et authentification renforcée (MFA, SAMLv2, FIDO2)

Adaptation aux environnements complexes

- Gestion multi-instances et multi-entités
- Adaptée aux grands groupes comme structures publiques ou privées
- Uniformisation des processus de gouvernance



"Nous utilisons Oodrive Meet pour tous nos conseils d'administration, afin que chacun, y compris les membres indépendants, ait un accès aussi rapide et sécurisé aux documents confidentiels dont il a besoin."

Jelle Jacquet
Chef adjoint du personnel, Orange Belgium

Conclusion : gouverner en toute confiance à l'ère numérique

À l'heure où les cybermenaces se sophistiquent et où la pression réglementaire s'intensifie, la gouvernance d'entreprise doit opérer une mue profonde. Les réunions stratégiques ne peuvent plus être organisées avec des pratiques artisanales ou des outils grand public. La sécurité numérique n'est plus un sujet technique : c'est un **enjeu stratégique et juridique** qui engage la responsabilité directe des dirigeants.

Oodrive Meet apporte une réponse concrète à cette transformation : une solution souveraine, certifiée et intuitive, qui concilie **fluidité d'organisation, protection des données sensibles** et **conformité réglementaire**.

Gouverner, c'est :

• Anticiper les risques plutôt que réagir aux crises ;
• Construire une culture commune de la sécurité de l'information ;
• S'appuyer sur des outils pensés pour les enjeux métier des conseils ;
• Garantir une gouvernance robuste et sereine, alignée sur les standards européens.

L'avenir de la gouvernance est numérique – mais il doit aussi être maîtrisé.

Ils nous font confiance

DANONE ONE PLANET. ONE HEALTH · CA · sanofi · LA POSTE GROUPE · orange · EDF · HERMÈS PARIS · SAFRAN · sodexo

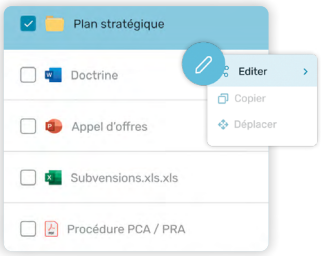
Suite collaborative souveraine et sécurisée

Qualifiée SecNumCloud depuis 2019 par l'ANSSI

Conçue pour les organisations publiques et privées, la suite Oodrive vous permet de collaborer en ligne en toute sécurité. Avec ses quatre solutions hébergées sur un cloud français sécurisé, elle garantit la confidentialité, l'intégrité et la conformité de vos données sensibles.

Collaboration sécurisée et souveraine

oodrive work



- Collaboration sécurisée
- Partage interne et externe
- Cyber Résilience PCA/PRA
- Diffusion restreinte

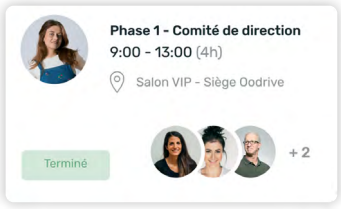
Signature électronique française

oodrive sign

- Conformité eIDAS
- Circuit de validation dématérialisé
- Hébergement qualifié SecNumCloud

Réunions dématérialisées

oodrive meet



- Instance de gouvernance digitalisée
- Visioconférence sécurisée

Conforme aux réglementations dès la conception

SecNumCloud	ISO 27001, 27701	HDS	Cloud souverain	Cloud au Centre	NIS 2	DORA
Qualifié depuis 2019 par l'ANSSI	Protection et sécurité de l'information garantie	Certifié Hébergeur de Données de Santé niveau 6/6	Oodrive est détenu et exploité en France	Conforme à la Doctrine Cloud au Centre	Conforme à la directive NIS 2	Conforme à la réglementation DORA

oodrive.com