DSCG • UE 5

# MANAGEMENT DES SYSTÈMES D’INFORMATION

SUJET ZÉRO

## DOCUMENT INSTITUTIONNEL

Extrait du Guide pédagogique 2026 et sujets zéro du DSCG, publié dans le cadre de l’accompagnement à la réforme du DSCG.

### SOURCES DU DOCUMENT

- Ministère de l’Enseignement supérieur, de la Recherche et de l’Espace
- Conseil national de l’Ordre des experts-comptables
- Compagnie nationale des commissaires aux comptes

La couverture a été ajoutée pour faciliter l’identification du fichier. Le contenu institutionnel reproduit dans les pages suivantes n’a pas été modifié.

# SUJET ZERO

UE5 – MANAGEMENT DES SYSTÈMES D'INFORMATION

Durée de l'épreuve : 3 heures Coefficient : 1

---

Document autorisé :

Aucun document ni aucun matériel n'est autorisé. En conséquence, tout usage d'une calculatrice est INTERDIT et constituerait une fraude.

Document remis au candidat :

Le sujet comporte 10 pages numérotées de 1 / 1 à 10 / 10.

Il vous est demandé de vérifier que le sujet est complet dès sa mise à votre disposition.

Le sujet se présente sous la forme de 3 dossiers indépendants :

DOSSIER 1 – GOUVERNANCE SI, IA ET PILOTAGE STRATÉGIQUE (16 points)
DOSSIER 2 – CYBERSÉCURITÉ AVANCÉE ET GESTION DES RISQUES SI (14 points)
DOSSIER 3 – DURABILITÉ NUMÉRIQUE, GREEN IT ET RSE (10 points)

Le sujet comporte 8 annexes :
Annexe 1 – Présentation de la SAS IAC-Digit et chiffres clés
Annexe 2 – Déploiement de l'IA générative : note d'orientation de la DSI
Annexe 3 – Architecture SI actuelle et chantiers du schéma directeur (extrait)
Annexe 4 – Repères réglementaires applicables (synthèse)
Annexe 5 – Évolution de la consommation énergétique du SI et impact de l'IA / Big Data
Annexe 6 – État des lieux de la cybersécurité (audit flash)
Annexe 7 – Témoignage d'un collaborateur : tentative d'hameçonnage (2024)
Annexe 8 – Empreinte carbone du SI et objectifs de durabilité 2027

---

AVERTISSEMENT

Si le texte du sujet, de ses questions ou de ses annexes vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement dans votre copie. Toutes les réponses devront être justifiées.

Il vous est demandé d'apporter un soin particulier à la présentation de votre copie et à la qualité rédactionnelle.

---

## SUJET

## LA SAS IAC-DIGIT À L'ÉPREUVE DE L'IA, DE LA CYBERSÉCURITÉ ET DE LA DURABILITÉ NUMÉRIQUE

Créée en 2022, la SAS IAC-Digit est née du regroupement de huit cabinets d'expertise comptable et de commissariat aux comptes, soucieux de mutualiser leurs systèmes d'information pour atteindre une taille critique face aux mutations de leur métier. Après une première phase consacrée à l'audit et à la sécurisation des SI des cabinets associés, la structure est aujourd'hui un prestataire de services SI à part entière, au service de huit cabinets, de quelque 620 collaborateurs et de plus de 10 000 PME et TPE clientes.

En 2027, la SAS IAC-Digit doit franchir une nouvelle étape de maturité. Trois mouvements de fond redéfinissent ses priorités :

- l'irruption de l'intelligence artificielle générative dans les processus comptables et de conseil, porteuse de gains de productivité mais aussi de risques inédits (hallucination, conformité au règlement européen sur l'IA, consommation énergétique) ;
- l'élévation continue du niveau de la menace cyber, qui impose de dépasser la défense périmétrique au profit d'une architecture de confiance (Zero Trust) et de se mettre en conformité avec la directive NIS2 ;
- la montée des obligations de durabilité (CSRD, normes ESRS) pesant sur les clients des cabinets, qui font de la donnée ESG et de la sobriété numérique des enjeux stratégiques.

Vous êtes membre de la direction des systèmes d'information de la SAS IAC-Digit. Le conseil de gouvernance vous confie une mission d'éclairage stratégique articulée autour de trois axes :

- définir la gouvernance du SI, encadrer le déploiement de l'IA et outiller le pilotage stratégique et extra-financier ;
- élever le niveau de cybersécurité et organiser la gestion des risques SI ;
- inscrire le SI dans une trajectoire de durabilité numérique et accompagner les clients soumis à la CSRD.

Pour conduire ce travail, vous vous appuierez sur les annexes fournies ainsi que sur vos connaissances professionnelles.

## DOSSIER 1 – GOUVERNANCE SI, IA ET PILOTAGE STRATÉGIQUE

La gouvernance du système d'information de la SAS IAC-Digit demeure embryonnaire, le dirigeant cumulant la fonction de directeur des SI. Le conseil de gouvernance souhaite professionnaliser le pilotage du SI, encadrer l'usage de l'intelligence artificielle et intégrer les enjeux de durabilité dans la stratégie numérique.

Vous mobiliserez pour cela les annexes 1, 2, 3, 4 et 8 ainsi que vos connaissances professionnelles.

**Q1 – Alignement stratégique, ESG et schéma directeur.**
a) Après avoir défini la notion d'alignement stratégique des systèmes d'information, montrez comment celui-ci doit évoluer pour intégrer les dimensions ESG et IA, et identifiez les principaux risques de désalignement auxquels la SAS IAC-Digit est exposée.
b) Proposez les grands axes d'un schéma directeur SI durable et sécurisé à horizon trois ans pour la SAS IAC-Digit.

**Q2 – Tableau de bord SI et indicateurs ESG.**
a) Présentez la structure d'un tableau de bord SI équilibré destiné à la direction, en y intégrant des indicateurs classiques (coûts, qualité, disponibilité) puis trois indicateurs ESG justifiés et contextualisés à partir de l'annexe 8.
b) Expliquez en quoi un tel tableau de bord SI peut contribuer au reporting CSRD des clients des cabinets membres.

**Q3 – IA générative : opportunités, limites et gouvernance.**
a) À partir de l'annexe 2, identifiez et argumentez trois opportunités majeures offertes par l'IA générative aux cabinets membres.
b) Analysez les principales limites et risques associés au déploiement de l'IA générative dans un contexte comptable et fiscal (hallucination, cadre réglementaire, biais, consommation énergétique).
c) Proposez une démarche de gouvernance de l'IA adaptée à la SAS IAC-Digit, en précisant les rôles, les processus de validation et les règles de contrôle.

**Q4 – Blockchain et traçabilité comptable.**
a) Présentez les apports de la technologie blockchain (registres distribués) pour la traçabilité et la fiabilité de l'information comptable.
b) Identifiez les principales limites opérationnelles de la blockchain et précisez le cadre réglementaire applicable (MiCA, NEP, ISO 22739).

## DOSSIER 2 – CYBERSÉCURITÉ AVANCÉE ET GESTION DES RISQUES SI

Le conseil de gouvernance de la SAS IAC-Digit vous confie la construction d'un plan global de sécurité pour l'ensemble des systèmes d'information mutualisés. Un audit flash a mis en évidence des vulnérabilités significatives, dans un contexte de menace renforcée par l'IA.

Vous mobiliserez pour cela les annexes 1, 4, 6 et 7 ainsi que vos connaissances professionnelles.

**Q5 – PSSI, PCA/PRA et rôle du RSSI.**
a) Définissez les trois propriétés de la triade CID (confidentialité, intégrité, disponibilité) et précisez leurs implications concrètes pour la SAS IAC-Digit.
b) Distinguez la PSSI, le PCA et le PRA, puis précisez la signification et des valeurs cibles cohérentes des indicateurs RTO et RPO dans le contexte des cabinets.
c) Caractérisez le rôle du RSSI et son positionnement dans la gouvernance de la SAS IAC-Digit.

**Q6 – IA dans les cyberattaques, BYOD et Zero Trust.**
a) À partir de l'annexe 7, présentez deux exemples d'utilisation de l'IA comme vecteur d'attaque, contextualisés au secteur de l'expertise comptable.
b) Montrez comment l'IA peut, à l'inverse, être mobilisée à des fins défensives pour la détection et la réponse aux incidents.
c) Analysez les risques spécifiques induits par le BYOD dans une architecture Zero Trust et proposez les mesures de contrôle adaptées.

**Q7 – Mesures Zero Trust enrichies et micro-segmentation.**
a) Proposez quatre mesures opérationnelles relevant d'une architecture Zero Trust. Pour chacune, vous préciserez le principe technique, sa pertinence pour la SAS IAC-Digit et un indicateur d'efficacité.
b) Expliquez comment la micro-segmentation et l'IAM contribuent à limiter les mouvements latéraux en cas de compromission.

**Q8 – Référentiels de cybersécurité et directive NIS2.**
a) Présentez deux référentiels ou normes de cybersécurité ou de gouvernance SI mobilisables par la SAS IAC-Digit, en précisant pour chacun son apport et sa pertinence.
b) Après avoir présenté le périmètre de la directive NIS2 (entités essentielles / entités importantes), analysez son applicabilité à la SAS IAC-Digit et les obligations qui en découleraient.

## DOSSIER 3 – DURABILITÉ NUMÉRIQUE, GREEN IT ET RSE

La SAS IAC-Digit entend inscrire son système d'information dans une trajectoire de sobriété et accompagner ses clients face aux obligations de durabilité. La première mesure de l'empreinte du SI vient d'être réalisée, dans un contexte de forte croissance des usages liés à l'IA et au Big Data.

Vous mobiliserez pour cela les annexes 1, 4, 5 et 8 ainsi que vos connaissances professionnelles.

**Q9 – Sobriété numérique et Green IT.**
a) Définissez les notions de sobriété numérique et de Green IT, et précisez l'enjeu stratégique qu'elles représentent pour la SAS IAC-Digit.
b) Proposez cinq actions Green IT couvrant au moins trois domaines distincts (matériel, hébergement, utilisateurs, logiciels). Pour chacune, précisez l'impact environnemental attendu et un indicateur de suivi.
c) À partir de l'annexe 5, analysez la tension entre performance technologique (IA, Big Data) et sobriété numérique, et proposez les principes d'une gouvernance SI permettant de la concilier.

**Q10 – CSRD, données ESG et rôle de la DSI.**
a) Présentez les exigences de la CSRD et des normes ESRS en matière de collecte, de traçabilité et de fiabilité des données ESG.
b) Identifiez deux rôles majeurs que la DSI de la SAS IAC-Digit peut assumer pour accompagner ses clients soumis à la CSRD (description, actions, outils).
c) Proposez une architecture SI ESG, identifiez les principaux risques relatifs à la qualité des données et précisez les contrôles associés.

**Q11 – Empreinte carbone du SI et maturité numérique durable.**
a) À partir de l'annexe 8, analysez l'évolution de l'empreinte carbone du SI et proposez une méthode de mesure ainsi qu'un plan de réduction.
b) Proposez une grille d'évaluation de la maturité numérique durable de la SAS IAC-Digit.

# ANNEXES

## Annexe 1 : Présentation de la SAS IAC-Digit et chiffres clés

Créée en 2022, la SAS IAC-Digit (Information, Audit & Conseil – Digit) est une structure de moyens mutualisée constituée par huit cabinets d'expertise comptable et de commissariat aux comptes implantés dans plusieurs régions françaises. Son objet est de consolider les systèmes d'information historiquement hétérogènes des cabinets fondateurs, de mutualiser les compétences numériques et de développer de nouvelles lignes de services à destination des clients.

Le dirigeant de la SAS assure également, à ce jour, la fonction de directeur des systèmes d'information, ce qui interroge la maturité de la gouvernance SI. La structure ambitionne, sur la période 2025-2028, de se positionner comme partenaire de la transformation numérique et durable de ses clients, en s'appuyant sur l'IA, la donnée et une trajectoire de cybersécurité et de sobriété renforcées.

| Indicateur | Valeur (2024) |
|---|---|
| Cabinets fondateurs regroupés | **8** |
| Effectif consolidé | **≈ 620 collaborateurs** |
| Chiffre d'affaires consolidé | **78 M€** |
| Total de bilan consolidé | **31 M€** |
| Portefeuille clients | **> 10 000 PME et TPE** |
| Budget SI annuel | **4,2 M€ (5,4 % du CA)** |
| Effectif de la DSI mutualisée | **12 ETP** |
| ERP / outils de production comptable | **3 éditeurs distincts (non unifiés)** |

## Annexe 2 : Déploiement de l'IA générative – note d'orientation de la DSI

*Note interne – Direction des systèmes d'information – Objet : usages prioritaires de l'IA générative.*

Plusieurs cabinets membres expérimentent depuis 2024 des outils d'IA générative. La DSI souhaite encadrer et prioriser ces usages. Quatre cas d'usage sont aujourd'hui à l'étude :

- Automatisation avancée de la saisie comptable : au-delà de la simple reconnaissance de caractères (OCR), proposition d'imputation

comptable contextuelle, détection d'anomalies et pré-contrôle des écritures. Gain de temps estimé par les chefs de mission entre 30 % et 40 % sur les tâches de saisie répétitives.

- Génération de commentaires et de synthèses : rédaction assistée de commentaires sur les comptes annuels, de projets de rapports de gestion et de notes de synthèse fiscale, le collaborateur passant d'une posture de production à une posture de supervision et de conseil.
- Détection proactive des risques de fraude : analyse comportementale des flux de transactions pour identifier des schémas inhabituels, envisagée comme un service différenciant à destination des PME clientes.
- Assistant de recherche documentaire fiscale et réglementaire : interrogation en langage naturel d'une base documentaire interne (doctrine, jurisprudence, NEP).

**Réserves exprimées par les associés :** fiabilité des résultats produits, responsabilité en cas d'erreur transmise au client, confidentialité des données clients, soumises aux outils et coût énergétique des traitements. Aucune charte d'utilisation n'existe à ce jour.

**Annexe 3 : Architecture SI actuelle et chantiers du schéma directeur (extrait)**

L'architecture issue du regroupement demeure partiellement consolidée. Les principaux constats sont les suivants :

- Production comptable : trois ERP/éditeurs coexistent selon les cabinets, sans référentiel commun de données (tiers, plans comptables, articles de TVA hétérogènes).
- Gestion documentaire : plusieurs GED distinctes, faible interopérabilité, recherche transverse impossible entre cabinets.
- Données : projet de Master Data Management (MDM) en cours de cadrage ; entrepôt de données (datawarehouse) à l'état de projet, non déployé ; pas de plateforme de collecte de données ESG.
- Hébergement : modèle hybride (cloud SaaS pour la production, serveurs internes pour la GED et les sauvegardes), sans politique d'hébergement formalisée.
- Décisionnel : reporting bureautique dispersé ; pas d'outil de Business Intelligence partagé.

**Chantiers identifiés pour le schéma directeur 2025-2028** : consolidation de la plateforme data (MDM, datawarehouse, qualité des données),

déploiement maîtrisé de l'IA, renforcement de la cybersécurité, et trajectoire de sobriété numérique.

## Annexe 4 : Repères réglementaires applicables (synthèse)

| Texte / cadre | Objet principal | Repère |
|---|---|---|
| CSRD / ESRS | **Reporting de durabilité audité ; extension progressive aux ETI puis aux PME ; exigence de fiabilité et de traçabilité des données ESG.** | **2022 – 2024+** |
| Règlement IA (AI Act) | **Classification des systèmes d'IA par niveau de risque ; obligations de transparence, de journalisation et de conformité pour les usages « à haut risque ».** | **2024+** |
| MiCA | **Encadrement de l'émission et des échanges de crypto-actifs dans l'UE ; enjeux de comptabilisation et de fiscalité.** | **2024** |
| NIS2 / loi CYBER | **Renforcement des obligations de cybersécurité ; distinction entités essentielles / importantes ; notification des incidents à l'ANSSI.** | **2024** |
| RGPD | **Protection des données à caractère personnel ; pertinent pour les données d'entraînement des modèles d'IA.** | **2018** |
| Loi REEN | **Réduction de l'empreinte environnementale du numérique ; appui des travaux ADEME / ARCEP.** | **2021** |

## Annexe 5 : Évolution de la consommation énergétique du SI et impact de l'IA / Big Data

La première campagne de mesure de la consommation énergétique du SI a été conduite sur l'année 2024 (aucune mesure n'existait auparavant). La consommation serveur trimestrielle a progressé de +35 % entre le premier et le quatrième trimestre, sous l'effet du déploiement de l'IA générative et des traitements Big Data.

| Trimestre 2024 | Conso. (MWh) | Commentaire |
|---|---|---|
| T1 | **31** | **Charge de référence (production comptable)** |
| T2 | **35** | **Premiers pilotes d'IA générative** |
| T3 | **40** | **Montée en charge Big Data et IA** |
| T4 | **42** | **Généralisation des pilotes (+35 % vs T1)** |
| Total 2024 | **148** | **Première mesure annuelle complète** |

**Repère :** une requête adressée à un grand modèle de langage (LLM) consomme en moyenne dix fois plus d'énergie qu'une recherche web classique (sources ADEME / Agence internationale de l'énergie).

### Annexe 6 : État des lieux de la cybersécurité (audit flash)

Un audit flash conduit fin 2024 a mis en évidence les vulnérabilités suivantes

- Identités dispersées entre les huit cabinets, sans annuaire unifié ; authentification multifacteur (MFA) déployée de manière partielle.
- BYOD non encadré dans trois cabinets : usage d'équipements personnels pour accéder aux dossiers clients, sans solution de gestion de flotte (MDM) ni conteneurisation.
- Absence de RSSI formellement désigné ; la fonction est aujourd'hui assurée de facto par le dirigeant-DSI.
- PCA et PRA non formalisés et jamais testés ; sauvegardes existantes mais sans procédure de restauration éprouvée.
- Segmentation réseau quasi inexistante (réseau « à plat ») exposant à des mouvements latéraux en cas de compromission.
- Culture de sécurité hétérogène : 40 % seulement des collaborateurs ont suivi une sensibilisation à la cybersécurité (cf. annexe 8).

### Annexe 7 : Témoignage d'un collaborateur – tentative d'hameçonnage (2024)

*Témoignage de Romain K., collaborateur confirmé, recueilli lors du retour d'expérience interne.*

*« En pleine période de clôtures fiscales, j'ai reçu un courriel parfaitement rédigé en français, reprenant à l'identique la charte graphique de notre éditeur de logiciel comptable. Le message m'invitait à valider en urgence une mise à jour de sécurité de mon compte, avec un lien qui imitait le portail habituel. Le ton, les formulations, jusqu'à la signature, tout semblait authentique : aucune des fautes grossières que l'on repère d'ordinaire. Quelques heures plus tard, un second message, cette fois au nom d'un client que je connais réellement, me demandait de modifier un RIB fournisseur. C'est la coïncidence des deux sollicitations, et la pression du calendrier, qui m'ont mis la puce à l'oreille. J'ai signalé l'incident, mais j'ai compris à quel point ces attaques étaient devenues crédibles. »*

### Annexe 8 : Empreinte carbone du SI et objectifs de durabilité 2027

Le tableau ci-dessous présente les premiers indicateurs de durabilité numérique mesurés en 2024 et les cibles fixées à horizon 2027. Aucun de ces indicateurs n'était suivi avant 2024

| Indicateur de durabilité numérique | Mesure 2024 | Cible 2027 |
|---|---|---|
| Empreinte carbone du SI ($tCO_2e$) | **62** | **< 45** |
| Consommation énergétique (MWh/an) | **148** | **< 120** |
| Taux d'équipements reconditionnés | **6 %** | **25 %** |
| Taux de virtualisation des charges | **48 %** | **80 %** |
| Part du cloud sur infrastructure verte | **20 %** | **70 %** |
| Couverture formation cybersécurité | **40 %** | **100 %** |
| Taux de conformité réglementaire (RGPD, NIS2, AI Act) | **55 %** | **100 %** |

La réduction visée de l'empreinte carbone (de 62 à moins de 45 $tCO_2e$) représente une baisse d'environ 27 % en trois ans, dans un contexte de montée en charge des usages liés à l'IA et au Big Data (cf. annexe 5).