DSCG • UE 5

MANAGEMENT DES SYSTÈMES D’INFORMATION

ÉLÉMENTS DE CORRIGÉ

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.

ELEMENTS DE CORRIGE

UE5 – Management des systèmes d'information

Sujet zéro

ÉLÉMENTS INDICATIFS DE CORRIGÉ ET DE BAREME

Afin que le jury national puisse se prononcer en toute équité, ce barème doit être respecté par toutes les commissions de correction

BARÈME GÉNÉRAL

N°	Dossier / Question	Points
D1	**Gouvernance SI, IA et pilotage stratégique**	**16 pts**
Q1	Alignement stratégique, ESG et schéma directeur	4 pts
Q2	Tableau de bord SI et indicateurs ESG	4 pts
Q3	IA générative : opportunités, limites et gouvernance	5 pts
Q4	Blockchain et traçabilité comptable	3 pts
D2	**Cybersécurité avancée et gestion des risques SI**	**14 pts**
Q5	PSSI, PCA/PRA et rôle du RSSI	4 pts
Q6	IA dans les cyberattaques et BYOD / Zero Trust	4 pts
Q7	Mesures Zero Trust enrichies	3 pts
Q8	NIS2 et référentiels de cybersécurité	3 pts
D3	**Durabilité numérique, Green IT et RSE**	**10 pts**
Q9	Sobriété numérique et Green IT	4 pts
Q10	CSRD, ESG et rôle de la DSI	4 pts
Q11	Empreinte carbone et maturité numérique	2 pts
	TOTAL	**40 pts**

Barème établi sur 40 points, ramené sur 20.

TABLEAU DE CORRESPONDANCE QUESTIONS – ANNEXES

Ce tableau permet au correcteur de vérifier que chaque réponse mobilise effectivement les annexes attendues. Les annexes indiquées sont strictement incluses dans la liste de pièces propre à chaque dossier (D1 : 1, 2, 3, 4, 8 — D2 : 1, 4, 6, 7 — D3 : 1, 4, 5, 8).

Question	Annexes mobilisées	Donnée(s) attendue(s) dans la réponse
Q1	1, 3, 4	Convergence des 8 cabinets ; chantiers du schéma directeur 2025-2028 ; cadres ESG / IA Act
Q2	8, 4	Trois indicateurs ESG issus de l'annexe 8 ; exigences CSRD
Q3	2, 4	Trois opportunités de l'annexe 2 ; IA Act
Q4	4, 3	MiCA / ISO 22739 / NEP ; intégration aux ERP existants
Q5	6, 1	Absence de RSSI et de PCA/PRA testé ; cloisonnement inter-cabinets
Q6	7, 6	Hameçonnage IA (témoignage Romain K.) ; BYOD non encadré
Q7	6	Identités dispersées ; réseau « à plat »
Q8	4, 1	NIS2 ; seuils de taille (> 50 sal., > 10 M€, > 10 000 PME)
Q9	5, 8, 4	Hausse +35 % / 148 MWh ; taux de reconditionnement 25 % ; loi REEN / CSRD
Q10	4, 1	CSRD / ESRS ; architecture ESG construite ex nihilo (annexe 3 hors périmètre D3)
Q11	8	Empreinte 62 → < 45 tCO_2e ; 148 → < 120 MWh

DOSSIER 1 – GOUVERNANCE SI, IA ET PILOTAGE STRATÉGIQUE (16 points)

Q1 – Alignement stratégique, ESG et schéma directeur 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §1.1 – Élaborer et aligner la stratégie des SI : intégration progressive des critères ESG et de durabilité ; notion de désalignement stratégique.
- §1.2 – Concevoir et piloter la gouvernance des SI : tableau de bord SI intégrant des critères ESG ; maturité numérique.
- §1.3 – Diagnostiquer et piloter l'évolution des architectures : intégrer l'IA dans la réflexion stratégique ; impacts des technologies émergentes.

Annexes mobilisées : Annexes 1, 3 et 4

Barème détaillé

Composante	Points
Q1a – Évolution de l'alignement stratégique + risques de désalignement (IA, ESG)	2 pts — ½ définition AS · ½ intégration ESG · ½ intégration IA · ½ risques de désalignement
Q1b – Schéma directeur SI durable et sécurisé (horizon 3 ans)	2 pts — ½ identification des axes · ½ ESG dans le SD · ½ sobriété numérique · ½ sécurité / IA

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Définition vague de l'alignement stratégique, absence des dimensions ESG ou IA, pas de schéma directeur.
1,5 – 2 pts	Satisfaisant	Alignement stratégique défini, une dimension (ESG ou IA) évoquée, schéma directeur ébauché.
2,5 – 3 pts	Très bon	Les deux dimensions intégrées, risques de désalignement identifiés, schéma directeur structuré mais peu contextualisé.
3,5 – 4 pts	Excellent	Réponse complète et contextualisée : évolution de l'AS articulant IA et ESG, risques précis, schéma directeur opérationnel intégrant sobriété et sécurité.

Réponse indicative

Q1a – Évolution de l'alignement stratégique

L'alignement stratégique (AS) désigne la mise en cohérence permanente entre la stratégie métier et la stratégie SI. Pour la SAS IAC-Digit, l'AS initial avait pour objet la convergence des SI hétérogènes des huit cabinets fondateurs (annexe 1). En 2027, il doit intégrer deux dimensions nouvelles :

- **Dimension ESG** : les obligations de reporting de durabilité (CSRD / ESRS) pesant sur les clients impliquent que le SI collecte, consolide et restitue des données ESG fiables. Le SI devient un levier de performance globale (triple bottom line) et non plus seulement de performance économique.
- **Dimension IA générative** : l'intégration d'outils d'IA dans les processus comptables modifie les flux de données, les rôles et les exigences de gouvernance. L'alignement doit anticiper les usages métiers, les risques associés (AI Act, annexe 4) et l'explicabilité.

Principaux risques de désalignement : emballement technologique (déploiement de l'IA avant la maturité des données), inadéquation des compétences internes, fragmentation des référentiels ESG, dépendance à des fournisseurs cloud non souverains.

Q1b – Schéma directeur SI durable et sécurisé (horizon 3 ans)

Le schéma directeur SI (SD-SI) planifie l'évolution du SI sur 3 à 5 ans en articulant priorités métiers, technologiques et organisationnelles. Pour la SAS IAC-Digit, le SD-SI 2025-2028 (annexe 3) s'articule autour de quatre axes :

- Consolidation de la plateforme data (MDM, datawarehouse ESG, qualité des données).
- Déploiement responsable de l'IA (gouvernance de l'IA, validation humaine, AI Act).
- Cybersécurité renforcée (Zero Trust enrichi, NIS2, RSSI structuré).
- Sobriété numérique (Green IT, empreinte carbone, éco-conception logicielle).

Réponses tolérées

- Référence au modèle de Henderson-Venkatraman valorisée si bien expliquée.
- Mention du CIGREF ou du référentiel DINUM pour le schéma directeur acceptable.
- Focus sur l'interopérabilité inter-cabinets valorisé si contextualisé.

Erreurs types

- Réduire l'alignement à la standardisation d'un ERP.
- Omettre la dimension ESG ou IA alors qu'elles sont explicitement requises.
- Confondre schéma directeur et plan de projet opérationnel.

Q2 – Tableau de bord SI et indicateurs ESG 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §1.2 – Construire un tableau de bord SI intégrant des critères ESG ; mesurer la maturité numérique.
- §2.2 – Exploiter les données pour la création de valeur ; piloter la performance par les données.
- §4.3 – Intégrer les enjeux RSE dans la gouvernance SI ; mesurer l'impact environnemental des SI.

Annexes mobilisées : Annexes 8 et 4

Barème détaillé

Composante	Points
Q2a – Structure du tableau de bord + indicateurs classiques (coûts, qualité, disponibilité)	1,5 pt — ½ structure équilibrée · ½ pertinence des indicateurs · ½ lien avec les annexes
Q2a – 3 indicateurs ESG justifiés et contextualisés	1,5 pt — ½ par indicateur (identification + justification)
Q2b – Lien avec le reporting CSRD des clients	1 pt — ½ rôle du SI dans le reporting CSRD · ½ valeur ajoutée pour les cabinets

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Tableau de bord réduit à des indicateurs techniques, aucun indicateur ESG, pas de lien CSRD.
1,5 – 2 pts	Satisfaisant	Structure équilibrée présente, 1 ou 2 indicateurs ESG évoqués sans justification.
2,5 – 3 pts	Très bon	Tableau de bord structuré, 3 indicateurs ESG identifiés et partiellement justifiés, lien CSRD ébauché.
3,5 – 4 pts	Excellent	Structure complète et équilibrée, 3 indicateurs ESG justifiés et contextualisés, lien clair avec la valeur ajoutée pour les clients CSRD.

Réponse indicative

Q2a - Structure du tableau de bord SI

Un tableau de bord SI équilibré repose sur quatre axes de pilotage, adaptés du Balanced Scorecard de Kaplan et Norton :

- Performance financière : TCO, budget SI / CA, retour sur investissement des projets SI.
- Qualité de service (SLA) : taux de disponibilité, délai moyen de résolution des incidents, taux de résolution N1 au premier contact.
- Projets et innovation : taux d'avancement, respect des délais et budgets, nombre de nouveaux services déployés.

- Durabilité et ESG (axe nouveau) : indicateurs environnementaux, sociaux et de gouvernance.

Trois indicateurs ESG pertinents, issus de l'annexe 8 :

- •Empreinte carbone du SI (tCO_2e) : impact environnemental direct ; cible 2027 < 45 tCO_2e. Lié à la sobriété numérique et aux obligations CSRD des clients.
- Taux de couverture de la formation cybersécurité (%) : indicateur social ; cible 2027 100 %. Le risque humain étant le 1er vecteur d'attaque, il contribue à la résilience collective.
- Taux de conformité réglementaire (RGPD, NIS2, AI Act) : indicateur de gouvernance ; cible 2027 100 %. Obligation légale et enjeu de réputation vis-à-vis des clients.

Q2b – Contribution au reporting CSRD des clients

La CSRD impose un rapport de durabilité selon les normes ESRS. Pour les PME clientes, la DSI peut jouer un rôle d'agrégateur de données ESG : connecteurs avec les ERP clients, plateforme de collecte ESG, tableaux de bord ESRS. Les cabinets se positionnent ainsi comme partenaires de la transformation durable de leurs clients, créant une ligne de services à forte valeur ajoutée.

Réponses tolérées

- Référence à des outils spécifiques (Power BI, Tableau, Greenspector) valorisée.
- Mention du GRI (Global Reporting Initiative) ou de l'EFRAG recevable.
- Indicateurs ESG différents acceptés s'ils sont justifiés et contextualisés.

Erreurs types

- Limiter le tableau de bord aux seuls indicateurs techniques.
- Évoquer la CSRD sans expliquer le rôle du SI dans la collecte et la fiabilisation des données.
- Proposer des indicateurs ESG génériques non applicables à une DSI.

Q3 – IA générative : opportunités, limites et gouvernance 5 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §1.3 – Comprendre les principes d'un modèle d'IA ; identifier les usages métiers (automatisation, aide à la décision) ; évaluer opportunités et limites.

- §1.3 – Préciser les limites actuelles (hallucination, biais, consommation énergétique) ; suivre les normes en évolution (IA Act).
- §4.1 – Risques liés à l'IA dans les attaques ; apport de l'IA pour limiter le risque.

Annexes mobilisées : Annexes 2 et 4

Barème détaillé

Composante	Points
Q3a – 3 opportunités majeures de l'IA générative	1,5 pt — ½ par opportunité identifiée et argumentée
Q3b – Limites et risques (hallucination, AI Act, biais, énergie)	2 pts — ½ par limite correctement expliquée et contextualisée
Q3c – Démarche de gouvernance de l'IA (rôles, processus, contrôle)	1,5 pt — ½ rôles · ½ processus de validation · ½ règles et contrôles

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Opportunités ou limites très générales, sans contextualisation, absence de gouvernance.
1,5 – 2,5 pts	Satisfaisant	2 opportunités et 2 limites présentées, gouvernance esquissée.
3 – 4 pts	Très bon	3 opportunités et 3-4 limites argumentées, gouvernance structurée mais incomplète sur le cadre réglementaire.
4,5 – 5 pts	Excellent	3 opportunités à impact métier, 4 limites incluant l'AI Act, gouvernance opérationnelle avec rôles et indicateurs de contrôle.

Réponse indicative

Q3a – Trois opportunités majeures (d'après l'annexe 2)

- Automatisation avancée de la saisie comptable : au-delà de l'OCR, imputation comptable contextuelle, détection d'anomalies, réduction du contrôle manuel ; gain de temps estimé à 30-40 %.
- Génération de commentaires et d'analyses clients : rédaction automatisée de commentaires, rapports de gestion, synthèses fiscales ; les collaborateurs passent de la production à la supervision et au conseil.
- Détection proactive des risques de fraude : analyse comportementale des transactions en temps réel ; service différenciant à forte valeur ajoutée pour les PME clientes.

Q3b – Limites et risques

- Hallucination (risque principal) : les LLM produisent des informations fausses mais vraisemblables ; en contexte comptable ou fiscal,

conséquences juridiques et financières. Validation humaine impérative.

- Règlement européen sur l'IA (AI Act, annexe 4) : classe certains systèmes en « haut risque » ; des usages comptables pourraient en relever (transparence, journalisation, évaluation de conformité).
- Biais et qualité des données : un modèle entraîné sur des données biaisées produit des résultats biaisés ; la gouvernance des données d'entraînement est un prérequis.
- Consommation énergétique : une requête LLM consomme ~10× une recherche web ; tension directe avec les objectifs de sobriété (annexe 5).

Q3c – Démarche de gouvernance de l'IA

- Rôles et responsabilités : désigner un référent IA, constituer un comité de validation (DSI, métier, juridique), définir les responsabilités en cas d'erreur imputable à l'IA.
- Processus de validation : aucun résultat IA transmis sans validation humaine ; circuit à deux niveaux (collaborateur + chef d'équipe) ; journalisation des utilisations.
- Règles et indicateurs de contrôle : charte d'utilisation opposable, indicateurs de suivi (taux d'erreur détecté, validations rejetées), audits périodiques des modèles.

Réponses tolérées

- Référence à des outils spécifiques (GitHub Copilot, ChatGPT, Claude) valorisée si contextualisée.
- Mention du RGPD en lien avec les données d'entraînement recevable.
- Approche comparative (IA forte vs IA étroite) acceptée si pertinente.

Erreurs types

- Confondre IA générative et machine learning classique.
- Omettre l'AI Act alors qu'il est au programme.
- Présenter les opportunités sans les risques, ou inversement.
- Proposer une gouvernance purement technique sans dimension organisationnelle.

Q4 – Blockchain et traçabilité comptable 3 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §1.3 – Intégrer les technologies de registres distribués dans la réflexion stratégique ; évaluer les impacts organisationnels, comptables et juridiques.
- §3.3 – Appréhender les usages et enjeux de la blockchain et des cryptoactifs ; analyser le cadre réglementaire (MiCA, NEP, ISO).

Annexes mobilisées : Annexes 4 et 3

Barème détaillé

Composante	Points
Q4a – Apports de la blockchain (immuabilité, transparence, smart contracts)	1,5 pt — ½ par apport pertinent et contextualisé
Q4b – Limites opérationnelles et cadre réglementaire (MiCA, NEP, ISO 22739)	1,5 pt — ½ limites · ½ réglementation · ½ contextualisation DSCG

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 0,5 pt	Insuffisant	Définition très vague, aucun lien avec la comptabilité, pas de réglementation.
1 pt	Satisfaisant	Principes généraux présentés, 1-2 apports, cadre réglementaire évoqué sans précision.
2 pts	Très bon	3 apports argumentés, limites évoquées, MiCA ou ISO 22739 mentionnés.
3 pts	Excellent	Apports contextualisés (traçabilité, smart contracts, audit continu), limites précises, cadre MiCA / NEP / ISO maîtrisé.

Réponse indicative

Q4a – Apports de la blockchain pour la comptabilité

- Immuabilité et traçabilité des écritures : chaque écriture est horodatée, signée et non modifiable rétroactivement ; intégrité renforcée et contrôles d'audit facilités.
- Smart contracts et automatisation : exécution automatique dès la réalisation de conditions prédéfinies (paiements fournisseurs, commissions) ; moins d'erreurs et de délais.
- Audit en quasi-temps réel : la transparence ouvre la perspective d'un audit continu, réduisant la dépendance aux audits périodiques.

Q4b – Limites et cadre réglementaire

Limites opérationnelles : scalabilité limitée des blockchains publiques, consommation énergétique (proof-of-work), complexité d'intégration avec les ERP existants (annexe 3), absence de norme comptable consolidée. Les NEP ne prévoient pas de méthodologie d'audit dédiée.

- Règlement MiCA (2024) : encadre l'émission et les échanges de cryptoactifs dans l'UE ; comptabilisation et fiscalité de ces actifs.

- ISO 22739 : terminologie de la technologie des registres distribués.
- Qualification juridique des smart contracts : incertitude persistante en droit français sur leur valeur contractuelle.

Réponses tolérées

- Mention de la blockchain privée (Hyperledger) vs publique (Ethereum) valorisée.
- Référence à des usages sectoriels (supply chain, finance décentralisée) recevable.
- Évocation de la facture électronique / du PISTE comme alternative centralisée pertinente.

Erreurs types

- Confondre blockchain et simple base de données distribuée.
- Présenter la blockchain comme immédiatement opérationnelle sans évoquer les obstacles d'intégration.
- Ignorer le cadre réglementaire MiCA alors qu'il est explicitement au programme.

DOSSIER 2 – CYBERSÉCURITÉ AVANCÉE ET GESTION DES RISQUES SI (14 points)

Q5 – PSSI, PCA/PRA et rôle du RSSI 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §4.1 – Intégrer la dimension risque dans la gouvernance SI ; assurer la conformité et la traçabilité du SI.
- §4.2 – Formaliser les procédures de sécurisation SI ; définir les responsabilités des acteurs ; intégrer la continuité d'activité dans la stratégie SI.

Annexes mobilisées : Annexes 6 et 1

Barème détaillé

Composante	Points
Q5a – Triade CID : définitions + implications contextualisées	1,5 pt — ½ par propriété (définition + implication)
Q5b – Articulation PSSI / PCA / PRA + RTO / RPO	1,5 pt — ½ PSSI · ½ distinction PCA/PRA · ½ RTO/RPO contextualisé
Q5c – Rôle du RSSI et articulation avec la gouvernance	1 pt — ½ missions · ½ positionnement

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Définitions vagues, PCA et PRA confondus, RSSI non mentionné.
1,5 – 2 pts	Satisfaisant	Triade CID définie, PCA/PRA distingués, RSSI évoqué sommairement.
2,5 – 3 pts	Très bon	Réponse structurée avec RTO/RPO, rôle du RSSI décrit, contextualisation partielle.
3,5 – 4 pts	Excellent	Triade CID avec implications concrètes, articulation PSSI/PCA/PRA avec RTO/RPO chiffrés, rôle et positionnement du RSSI précis.

Réponse indicative

Q5a – La triade CID

- Confidentialité : seules les personnes autorisées accèdent aux données (MFA, chiffrement au repos et en transit, RBAC). Pour la SAS : cloisonnement des données clients entre cabinets (annexe 1).
- Intégrité : les données restent exactes et non altérées (journalisation, contrôles de cohérence, sauvegardes avec hash, validation des écritures). Enjeu critique en comptabilité.
- Disponibilité : accès aux systèmes au moment voulu (redondance, PCA/PRA, SLA SaaS, tests de basculement).

Q5b – PSSI, PCA et PRA

La PSSI est le document cadre énonçant objectifs, règles et responsabilités ; elle est le référentiel à partir duquel s'articulent PCA et PRA. Le PCA maintient un service minimal en mode dégradé ; le PRA organise le retour à la normale après sinistre.

- RTO (Recovery Time Objective) : durée maximale d'interruption acceptable ; pour les cabinets, < 4 heures en période fiscale.
- RPO (Recovery Point Objective) : perte de données maximale admissible ; pour des données comptables, ≤ 24 heures.

Q5c – Rôle du RSSI

Le RSSI est le garant de la politique de cybersécurité : définir et maintenir la PSSI, piloter les audits, gérer les incidents, assurer la veille réglementaire, animer la culture de sécurité. L'annexe 6 souligne l'absence de RSSI désigné : il doit être positionné en lien direct avec la direction (PDG-DSI) et disposer d'une autorité fonctionnelle sur l'ensemble des cabinets.

Réponses tolérées

- Mention de la norme ISO 27001 et du SMSI valorisée.
- Traçabilité comme 4e propriété recevable si bien définie.

- Chiffres RTO/RPO différents acceptés si cohérents avec le contexte des cabinets.

Erreurs types

- Confondre PCA et PRA.
- Décrire le RSSI comme un simple technicien informatique.
- Omettre les RTO/RPO.

Q6 – IA dans les cyberattaques, BYOD et Zero Trust 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §4.1 – Risques liés à l'IA dans les attaques ; apport de l'IA pour limiter le risque ; cadre réglementaire (cybersécurité).
- §4.2 – Appréhender les notions d'architecture de confiance ; présenter les dispositifs de surveillance (IAM, UEBA) ; responsabilités dans la gestion des SI critiques.

Annexes mobilisées : Annexes 7 et 6

Barème détaillé

Composante	Points
Q6a – IA comme vecteur d'attaque : 2 exemples contextualisés	1 pt — ½ par exemple (type d'attaque + illustration comptable)
Q6b – IA défensive : détection et réponse aux incidents	1 pt — ½ par apport défensif contextualisé
Q6c – Risques BYOD en Zero Trust + mesures	2 pts — 1 analyse des risques · 1 mesures de contrôle adaptées

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Attaques IA très générales, BYOD/ZT non articulés, mesures absentes.
1,5 – 2 pts	Satisfaisant	1 exemple d'attaque, 1 apport défensif, risques BYOD sans mesures.
2,5 – 3 pts	Très bon	2 exemples pertinents, apports défensifs décrits, risques BYOD/ZT analysés, mesures esquissées.
3,5 – 4 pts	Excellent	2 exemples contextualisés, IA défensive articulée (UEBA/SIEM), risques BYOD précis, mesures opérationnelles (MDM, accès conditionnel, certification terminaux).

Réponse indicative

Q6a – IA comme vecteur d'attaque (d'après l'annexe 7)

- Hameçonnage augmenté par l'IA : courriels parfaitement rédigés imitant l'éditeur SaaS ou un client connu, personnalisables à

l'échelle (spear phishing). Le témoignage de Romain K. (annexe 7) illustre une tentative réelle en 2024.

- Rançongiciel automatisé par l'IA : reconnaissance automatisée des cibles, identification des fichiers comptables prioritaires, adaptation de la rançon ; la pression des clôtures fiscales est aggravante.

Q6b – IA défensive

- UEBA (User and Entity Behavior Analytics) : analyse comportementale en temps réel ; détecte les anomalies (connexion hors horaires, volumes inhabituels) même d'utilisateurs authentifiés. Complément du Zero Trust.
- SIEM augmenté par l'IA : corrélation automatique des événements, priorisation des alertes, réduction des faux positifs ; allège le SOC et accélère la réponse.

Q6c – Risques BYOD et mesures Zero Trust

En architecture Zero Trust, le BYOD génère des risques spécifiques (annexe 6) : impossibilité de garantir la conformité du terminal, mélange données pro/perso, applications tierces non contrôlées, difficulté d'appliquer le MDM sur des équipements non propriétaires.

- Accès conditionnel : refuser l'accès si le terminal ne satisfait pas aux critères (OS à jour, antivirus actif, chiffrement).
- MDM avec conteneurisation : isoler les données pro dans un conteneur chiffré, effaçable à distance.
- Certification des terminaux : enregistrement préalable dans le répertoire d'identités (Entra ID / Active Directory) avant tout accès.

<u>Réponses tolérées</u>

- Mention d'outils spécifiques (Defender, CrowdStrike, Sentinel) valorisée.
- Référence au BYOA (Bring Your Own Application) pertinente si contextualisée.
- Évocation des deepfakes audio/vidéo comme vecteur d'attaque BtoB recevable.

<u>Erreurs types</u>

- Réduire le BYOD à un simple problème de virus.
- Présenter le Zero Trust comme une réponse à tous les risques sans nuance.
- Confondre MDM et MAM (Mobile Application Management).

Q7 – Mesures Zero Trust enrichies et micro-segmentation 3 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §4.2 – Concevoir, mettre en œuvre et contrôler une politique de cybersécurité ; dispositifs de surveillance (IAM, PCA/PRA) ; architecture de confiance.

Annexes mobilisées : Annexe 6

Barème détaillé

Composante	Points
Q7a – 4 mesures Zero Trust (principe + pertinence + indicateur)	2 pts — ½ par mesure complète
Q7b – Micro-segmentation et IAM contre les mouvements latéraux	1 pt — ½ micro-segmentation · ½ IAM + articulation

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 0,5 pt	Insuffisant	Mesures vagues ou hors sujet, micro-segmentation/IAM absents.
1 pt	Satisfaisant	2 mesures identifiées, explications partielles, micro-segmentation ou IAM évoqué.
2 pts	Très bon	3-4 mesures correctes avec principe, micro-segmentation ET IAM décrits.
3 pts	Excellent	4 mesures complètes (principe + pertinence + indicateur), articulation micro-segmentation / IAM claire.

Réponse indicative

Q7a – Quatre mesures opérationnelles Zero Trust

- IAM / MFA / RBAC : identités centralisées, MFA, contrôle d'accès par rôle. Pertinence : dispersion actuelle des identifiants (annexe 6). Indicateur : taux de connexions sans MFA (cible 0 %).
- MDM / EDR sur tous les terminaux (y compris BYOD) : gestion des terminaux et détection des menaces. Pertinence : équipements personnels non contrôlés. Indicateur : taux de terminaux conformes (cible 100 %).
- Accès conditionnel et gestion des sessions : vérification dynamique du contexte (localisation, horaire) à chaque accès. Pertinence : travail à distance et multi-sites. Indicateur : sessions rejetées pour non-conformité.

- UEBA / SIEM comportemental : surveillance des comportements post-authentification. Pertinence : menaces internes et comptes compromis. Indicateur : délai moyen de détection (MTTD).

Q7b – Micro-segmentation et IAM contre les mouvements latéraux

La micro-segmentation divise le réseau en zones granulaires (données clients, infrastructure DSI, GED, accès externes) ; en cas de compromission, l'attaquant ne peut se déplacer librement. L'annexe 6 relève un réseau « à plat », d'où la pertinence. L'IAM complète le dispositif (moindre privilège). Micro-segmentation + IAM + UEBA forment le triptyque du Zero Trust mature.

Réponses tolérées

- Mesures différentes recevables si principe, pertinence et indicateur sont présents.
- Référence à des solutions spécifiques (Microsoft Entra, Palo Alto, CrowdStrike) valorisée si contextualisée.

Erreurs types

- Mesures redondantes (ex. MFA + MFA bis).
- Absence des indicateurs d'efficacité.
- Confondre micro-segmentation réseau et segmentation applicative.

Q8 – Référentiels de cybersécurité et directive NIS2 3 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §3.2 – Connaître les référentiels d'audit (COBIT, ITIL, NEP, ISO) ; réaliser un audit des processus SI ; formuler des recommandations.
- §4.1 – Appréhender les enjeux éthiques et réglementaires ; assurer la conformité et la traçabilité du SI.
- §4.2 – Cadres réglementaires liés à la gestion du risque.

Annexes mobilisées : Annexes 4 et 1

Barème détaillé

Composante	Points
Q8a – 2 référentiels : identification + utilité + contextualisation	1,5 pt — ½ + ½ par référentiel
Q8b – NIS2 : périmètre, catégories EE/EI, obligations	1,5 pt — ½ catégories · ½ application à la SAS · ½ obligations concrètes

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 0,5 pt	Insuffisant	Référentiels non identifiés ou confondus, NIS2 absente ou très vague.
1 pt	Satisfaisant	1 référentiel correct, NIS2 évoquée sans analyse d'applicabilité.
2 pts	Très bon	2 référentiels contextualisés, NIS2 définie avec catégories EE/EI.
3 pts	Excellent	2 référentiels (identification, apport, pertinence), analyse précise de l'applicabilité de NIS2 à la SAS et obligations associées.

Réponse indicative

Q8a – Deux référentiels mobilisables

- ISO 27001 (SMSI) : norme certifiable structurant un Système de Management de la Sécurité de l'Information selon un cycle PDCA ; cadre homogène applicable à l'ensemble des cabinets, auditable.
- COBIT 2019 (gouvernance SI) : cadre structurant les processus en cinq domaines (EDM, APO, BAI, DSS, MEA) ; évalue la maturité et définit une trajectoire de convergence mesurable.

Q8b – Directive NIS2 et applicabilité à la SAS IAC-Digit

NIS2 (transposée en France en 2024, annexe 4) distingue deux catégories :

- Entités Essentielles (EE) : secteurs critiques (énergie, transport, banque, santé, infrastructure numérique). Les cabinets n'en relèvent pas a priori.
- Entités Importantes (EI) : périmètre élargi incluant des prestataires de services numériques. La SAS IAC-Digit, prestataire SI mutualisé gérant les données de plus de 10 000 PME, pourrait être qualifiée d'EI au regard des seuils de taille (> 50 salariés, > 10 M€ de CA — annexe 1).

Obligations pour une EI : gestion des risques cyber (politique, gestion des incidents, continuité), notification des incidents significatifs à l'ANSSI sous 24 heures, audit de conformité, responsabilité des dirigeants en cas de manquement.

Réponses tolérées

- NIST Cybersecurity Framework (CSF) recevable si bien présenté.
- Référence à l'ANSSI et à ses guides méthodologiques valorisée.
- Mention du DORA acceptable si le lien avec les clients financiers est fait.

Erreurs types

- Présenter ISO 27001 comme une simple checklist technique.

- Affirmer catégoriquement que NIS2 ne s'applique pas sans analyse.
- Confondre NIS2 et RGPD.

DOSSIER 3 – DURABILITÉ NUMÉRIQUE, GREEN IT ET RSE (10 points)

Q9 – Sobriété numérique et Green IT 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §4.3 – Assurer une veille sur les cadres réglementaires (CSRD, ESRS) ; appliquer les pratiques Green IT ; mesurer l'empreinte carbone d'un SI ; intégrer la durabilité dans la stratégie SI.

Annexes mobilisées : Annexes 5, 8 et 4

Barème détaillé

Composante	Points
Q9a – Définitions sobriété / Green IT + enjeu stratégique	1 pt — ½ définitions · ½ enjeu contextualisé
Q9b – 5 actions Green IT (impact + indicateur), ≥ 3 domaines	2 pts — ½ par action complète
Q9c – Tension performance / sobriété et gouvernance responsable	1 pt — ½ tension IA/sobriété · ½ gouvernance de conciliation

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	Définitions absentes ou confuses, actions génériques, tension IA/sobriété non abordée.
1,5 – 2 pts	Satisfaisant	Définitions correctes, 3 actions avec impact, tension évoquée.
2,5 – 3 pts	Très bon	5 actions avec impact, 3 domaines couverts, tension analysée, gouvernance esquissée.
3,5 – 4 pts	Excellent	Définitions précises, 5 actions avec impact ET indicateur, tension analysée avec l'annexe 5, gouvernance responsable opérationnelle.

Réponse indicative

Q9a – Définitions

- Sobriété numérique : réduire l'empreinte environnementale du numérique par un usage raisonné, en questionnant la nécessité de chaque usage.
- Green IT : pratiques visant à concevoir, produire, utiliser et recycler les équipements et infrastructures de manière plus respectueuse de l'environnement.

Enjeu stratégique pour la SAS : réduire les coûts d'exploitation et répondre aux attentes RSE des clients, notamment ceux soumis à la CSRD (annexe 4) qui doivent reporter leur empreinte numérique.

Q9b – Cinq actions Green IT

- Allongement de la durée de vie des équipements (matériel) : reconditionné et cycle de vie ≥ 5 ans. Impact : −25 à −30 % d'émissions de fabrication. Indicateur : taux d'équipements reconditionnés (cible 25 %, annexe 8).
- Virtualisation et consolidation des serveurs (hébergement) : Impact : −20 à −40 % d'électricité. Indicateur : taux de virtualisation des charges.
- Datacenter à énergie renouvelable (hébergement cloud) : fournisseurs certifiés ISO 50001 ou à faible PUE. Indicateur : part du cloud sur infrastructure verte (%).
- Formation des utilisateurs aux gestes sobres (utilisateurs) : gestion des mails, visioconférence sobre, stockage raisonné. Impact : −5 à −10 %. Indicateur : taux de collaborateurs formés (cible 100 %).
- Éco-conception des applications (logiciels) : critères de performance énergétique dans les appels d'offres ; applications web légères. Indicateur : score Lighthouse / empreinte carbone de page.

Q9c – Tension performance / sobriété

L'annexe 5 l'illustre : la consommation serveur a progressé de +35 % entre T1 et T4 2024 (148 MWh sur l'année), sous l'effet de l'IA et du Big Data, une requête LLM consommant ~10× une recherche web. Pour concilier : (1) évaluer le rapport valeur créée / empreinte avant tout déploiement IA ; (2) privilégier les modèles frugaux (SLM, IA on-premise) ; (3) compenser les nouvelles émissions par des réductions Green IT mesurées ; (4) intégrer l'empreinte carbone au tableau de bord SI et aux arbitrages budgétaires.

Réponses tolérées

- Référence à la loi REEN (2021) ou au rapport ADEME / ARCEP valorisée.
- Mention du principe de double matérialité (CSRD) en lien avec l'empreinte numérique recevable.
- Autres actions Green IT recevables si elles couvrent des domaines distincts.

Erreurs types

- Confondre sobriété numérique et simple économie d'énergie.

- Proposer uniquement des gestes utilisateurs sans leviers infrastructurels.
- Ignorer la tension IA / sobriété, au cœur du programme.

Q10 – CSRD, données ESG et rôle de la DSI 4 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §2.3 – Appréhender les enjeux stratégiques de la donnée ; piloter la gouvernance de l'information ; garantir la conformité et la valeur des actifs numériques.
- §4.3 – Intégrer les enjeux RSE dans la gouvernance SI ; accompagner la transformation numérique responsable.

Annexes mobilisées : Annexes 4 et 1

Barème détaillé

Composante	Points
Q10a – Exigences CSRD/ESRS (collecte, traçabilité, fiabilité)	1 pt — ½ périmètre CSRD · ½ qualité des données ESG
Q10b – 2 rôles de la DSI pour accompagner les clients CSRD	1,5 pt — ½ + ½ par rôle · ½ valeur ajoutée pour les cabinets
Q10c – Architecture SI ESG + risques qualité + contrôles	1,5 pt — ½ architecture · ½ risques qualité · ½ contrôles

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 1 pt	Insuffisant	CSRD définie vaguement, rôles génériques, architecture absente.
1,5 – 2 pts	Satisfaisant	CSRD/ESRS compris, 1 rôle décrit, architecture esquissée sans risques.
2,5 – 3 pts	Très bon	2 rôles bien décrits avec outils, architecture fonctionnelle, risques évoqués.
3,5 – 4 pts	Excellent	CSRD/ESRS maîtrisés, 2 rôles opérationnels, architecture complète (IoT-ERP-ETL-DWH-BI), risques précis et contrôles associés.

Réponse indicative

Q10a – Exigences CSRD / ESRS

La CSRD (2022/2464) impose, au-delà de certains seuils (250 salariés, 50 M€ de CA ou 25 M€ de bilan), un rapport de durabilité audité selon les normes ESRS ; les PME y seront progressivement soumises (2026-2028, annexe 4). Exigences SI : données ESG collectées systématiquement, tracées (sources et méthodes de calcul), vérifiables par un OTI, comparables dans le temps. La qualité des données ESG est le premier obstacle.

Q10b – Deux rôles majeurs de la DSI

- Architecte de la collecte ESG : connecteurs vers les systèmes sources clients (ERP, compteurs, RH, IoT), entrepôt ESG structuré selon les axes ESRS, tableaux de bord. Actions : appels d'offres SI ESG, intégration API, MDM des données de référence.
- Garant de la qualité et de la traçabilité : contrôles qualité (exhaustivité, exactitude, cohérence temporelle), traçabilité (journalisation des sources, transformations, versions), piste d'audit pour l'OTI, formation des collaborateurs.

Cette double posture positionne les cabinets comme partenaires crédibles de la transformation durable de leurs clients PME.

Q10c – Architecture SI ESG et risques qualité

Architecture proposée (construite à partir des connaissances et du contexte de l'annexe 1) en quatre couches : sources (ERP, RH/paie, capteurs IoT, déchets, données financières) ; couche ETL (normalisation ESRS) ; entrepôt ESG (stockage versionné, piste d'audit) ; restitution (tableaux de bord Power BI / Tableau, rapports ESRS, interfaces OTI).

Risques qualité : hétérogénéité des sources, saisies manuelles non contrôlées, données estimées non documentées, ruptures temporelles. Contrôles : règles de validation à l'import, rapprochements croisés, alertes automatiques, validation par un responsable données ESG dans chaque cabinet.

Réponses tolérées

- Référence aux normes GRI ou TCFD recevable.
- Mention de la double matérialité (financière + d'impact) valorisée.
- Architecture SI différente recevable si les quatre couches fonctionnelles sont présentes.

Erreurs types

- Réduire la CSRD à une simple obligation de rapport annuel.
- Confondre le rôle de la DSI avec celui du commissaire aux comptes ou de l'OTI.
- Ignorer la dimension qualité des données, au cœur des ESRS.

Q11 – Empreinte carbone du SI et maturité numérique durable 2 points

Référence au programme (réforme 2025 – 1re application session 2027)

- §4.3 – Appliquer les pratiques Green IT ; mesurer l'empreinte carbone d'un SI ; intégrer la durabilité dans la stratégie SI.

Annexes mobilisées : Annexe 8

Barème détaillé

Composante	Points
Q11a – Analyse de l'annexe 8 + méthode de mesure et réduction	1 pt — ½ analyse des données · ½ méthode et plan de réduction
Q11b – Grille d'évaluation de la maturité numérique durable	1 pt — ½ dimensions pertinentes · ½ niveaux différenciés

Gradation de la notation

Fourchette	Niveau	Descriptif
0 – 0,5 pt	Insuffisant	Annexe 8 non exploitée, méthode absente, grille vague.
1 pt	Satisfaisant	Quelques données commentées, méthode ou grille esquissée.
1,5 pt	Très bon	Analyse pertinente, méthode de réduction opérationnelle, grille structurée.
2 pts	Excellent	Analyse chiffrée de l'annexe 8, plan de réduction progressif, grille sur 4+ dimensions avec niveaux différenciés.

Réponse indicative

Q11a – Analyse de l'annexe 8 et plan de réduction

L'annexe 8 montre l'absence de mesure avant 2024 ; la première mesure (62 tCO_2e, 148 MWh) constitue une baseline. La cible 2027 (< 45 tCO_2e, < 120 MWh) représente une réduction d'environ 27 % en trois ans, ambitieuse mais atteignable.

Méthode : Bilan Carbone® (ADEME) ou GHG Protocol, couvrant les scopes 1 (émissions directes), 2 (énergie achetée) et 3 (fabrication des équipements, déplacements IT, cloud). Plan progressif : an 1 → mesure et baselines par périmètre ; an 2 → actions matériel et hébergement (−15 %) ; an 3 → formation et éco-conception (−12 % supplémentaires).

Q11b – Grille de maturité numérique durable

Cinq dimensions évaluées sur 4 niveaux (Initial → Géré → Défini → Optimisé) :

- Mesure et reporting : de l'absence de mesure à un reporting ESG-SI intégré au rapport de durabilité.
- Pratiques Green IT : de l'absence de politique à un plan certifié avec indicateurs.
- Gouvernance SI durable : de l'absence de comité à un comité Durabilité Numérique intégré au Conseil de gouvernance.

- Compétences et culture : de la sensibilisation ponctuelle à une culture intégrée aux objectifs individuels.
- Sobriété des usages : de l'absence de guide à une charte du numérique responsable opposable et auditée.

Réponses tolérées

- Référence au référentiel GreenIT.fr ou au label Numérique Responsable recevable.
- Grille à 3 ou 5 niveaux recevable si les niveaux sont différenciés.
- Référence à l'indicateur PUE des datacenters valorisée.

Erreurs types

- Limiter l'analyse de l'annexe 8 à une simple lecture des chiffres.
- Proposer une grille sans niveaux différenciés (descriptif plat).
- Ignorer les données de l'annexe 8 alors que la question y fait référence