DSCG • UE 5

MANAGEMENT DES SYSTÈMES D’INFORMATION

GUIDE PÉDAGOGIQUE

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.

UE 5 – Management des systèmes d'information

GUIDE PEDAGOGIQUE

Ce guide de l'UE5 rassemble en un seul volume l'ensemble des outils élaborés pour accompagner la prise en main du nouveau référentiel de l'UE5 — Management des Systèmes d'Information du DSCG, applicable depuis la session de septembre 2025 et conforme à la fiche RNCP40998. Il est conçu pour être à la fois un outil de cadrage en début d'année, un compagnon de travail au fil des séances et un support de dialogue entre enseignants au sein des équipes pédagogiques.

- **Une structure en quatre pièces articulées**

Le document s'organise en quatre ensembles complémentaires, qui peuvent se lire indépendamment mais qui prennent tout leur sens lus ensemble :

- Le premier ensemble restitue le programme officiel et le décline en ressources opérationnelles. Pour chacune des 15 sous-sections du référentiel, l'enseignant trouvera d'une part une sélection commentée de six à huit références pédagogiques (manuels, articles, MOOC, rapports institutionnels) directement exploitables, d'autre part une proposition de démarche pédagogique en classe comportant un schéma séquencé et un cas pratique calibré sur le format des épreuves. C'est le cœur du guide, la pièce dans laquelle les enseignants reviendront le plus souvent au long de l'année.
- Le deuxième ensemble propose un inventaire complet des référentiels normatifs mobilisables (84 cadres distincts répartis en 10 catégories thématiques, depuis les normes professionnelles d'audit jusqu'aux référentiels de durabilité numérique) accompagné d'une matrice croisée référentiels × sous-sections qui permet d'identifier rapidement quel cadre mobiliser pour quel objectif d'apprentissage. Cette matrice est aussi un outil de cohérence : elle révèle les notions transversales qui irriguent plusieurs parties du programme et invite à construire des passerelles plutôt que des cloisonnements.
- Le troisième ensemble articule explicitement le programme avec les six compétences certifiées du bloc RNCP40998 BC05. Pour chaque compétence, une fiche détaillée précise sa formulation officielle, les sous-sections qu'elle couvre, les référentiels mobilisables et propose trois archétypes de situations professionnelles évaluables. C'est l'outil de pilotage par compétences, particulièrement utile pour calibrer les évaluations en cours d'année et anticiper les attendus du jury national.

- Le quatrième ensemble offre une vision synoptique en trois lectures complémentaires (un schéma vertical de la séquence pédagogique, une frise chronologique sur vingt-huit semaines, une vue par compétences transversales) pensé comme un support de réunion d'équipe et d'animation pédagogique.

Le glossaire et la bibliographie consolidée placés en fin de document servent de référence transverse à l'ensemble. Le glossaire intègre les entrées du CyberDico de l'ANSSI, sous licence Etalab. La bibliographie consolidée privilégie les ressources en accès libre afin que chacun puisse y accéder sans contrainte d'abonnement.

- **L'esprit du document**

Trois principes ont guidé sa construction :

- D'abord la primauté de l'usage : chaque outil a été pensé en partant d'une question concrète d'enseignant : comment cadrer une séance, choisir une ressource, construire un cas, calibrer une évaluation, plutôt que d'une logique d'exhaustivité documentaire.
- Ensuite la traçabilité de l'approche par compétences : la fiche RNCP n'est pas un document administratif à respecter en parallèle du programme, c'est la grille de lecture qui donne son sens à la trame ministérielle ; le guide rend cette articulation explicite à chaque étape.
- Enfin l'ouverture aux choix pédagogiques de chaque équipe : le programme officiel laisse délibérément aux enseignants la liberté de choisir les outils logiciels, les cas et les approches qui correspondent à leur contexte ; ce guide propose des chemins balisés sans prétendre les imposer.

Présentation du programme

La nouvelle version du programme reprend tous les éléments de l'ancienne version, seuls certains éléments qui étaient déjà vus dans l'UE 8 du DCG et le sont encore ne sont pas repris dans le présent programme.

Le programme est densifié et se développe en ajoutant des connaissances et compétences relatives à l'analyse des données, leur manipulation, la sécurité (cybersécurité) et des compétences relatives à l'utilisation de solutions logicielles. La durabilité apparaît comme une dimension transverse au travers des différentes parties (indicateurs de durabilité, durabilité vue comme une question de sécurité, durabilité dans la gouvernance...).

La démarche de management des SI est essentiellement une démarche visant à prendre du recul par rapport au système d'information dans ses

dimensions stratégiques et organisationnelles. Plusieurs points méritent d'être notés :

- La masse des éléments techniques à maîtriser est telle qu'il est impossible de tout reporter vers le DCG.
- Dans certains cas, la composante technique prend le pas sur le management : la compréhension de certaines configurations ou organisations repose plus sur une compréhension technique que sur des connaissances managériales classiques.

Trois compétences techniques transversales émergent du référentiel du Conseil National de l'Ordre : la capacité à mettre en place des analyses de données, la capacité à simuler des scénarios, et la capacité à manipuler des données. La formation des étudiants gagnera à être complétée par une initiation à des compétences en algorithmique au service de la manipulation de données, de la construction de scénarios et de l'analyse de données — étant entendu que le choix des outils et des cas reste à l'initiative de chaque équipe pédagogique.

- **Objectif général de l'UE5**

L'UE5 a pour objectif de doter les futurs experts-comptables des compétences nécessaires pour analyser, conseiller et accompagner les organisations dans le pilotage, la sécurisation et l'évolution des systèmes d'information (SI), dans une perspective de performance, de conformité et de création de valeur. Elle permet aux candidats de comprendre les enjeux stratégiques liés aux SI, d'en évaluer les risques, d'en accompagner la transformation, et d'en garantir l'alignement avec les modèles d'affaires et les objectifs de l'organisation. L'enseignement vise à mobiliser des méthodes et outils d'aide à la décision pour optimiser les processus, renforcer la gouvernance des SI, et anticiper les impacts des mutations technologiques, réglementaires et managériales. Cette UE articule ainsi les dimensions techniques, organisationnelles et éthiques des systèmes d'information, dans un contexte de transition numérique et de complexification des environnements professionnels.

- **Prérequis**

Le programme des UE 7 et 8 du DCG doit être maîtrisé. Les compétences, connaissances et savoirs associés qui y sont développés seront mobilisés à travers les compétences développées ci-dessous, à tous les niveaux.

- **Compétences transversales**

Les candidats seront en mesure de structurer, optimiser et animer les éléments d'un cahier des charges, d'aligner les SI avec la stratégie de l'organisation, d'intégrer les SI dans la stratégie globale pour soutenir les

objectifs organisationnels, de maîtriser les concepts, outils et techniques SI, d'adapter ces outils au contexte spécifique pour soutenir les décisions stratégiques et optimiser les processus de contrôle de gestion. Ils sauront accompagner le client dans son pilotage de la performance globale des SI à l'aide d'indicateurs adaptés, gérer les relations contractuelles avec les ESN, identifier et gérer les risques de cybersécurité, et analyser des situations complexes pour formuler des préconisations communiquées de manière structurée, en tenant compte des enjeux technologiques.

- **Le référentiel**

Le programme s'organise globalement de la manière suivante :

- On définit une stratégie (Partie 1, 24 heures)
- On organise et exploite la donnée (Partie 2, 48 heures)
- On mesure la performance (Partie 3, 32 heures)
- On sécurise et pérennise (Partie 4, 36 heures)

Le programme totalise ainsi 140 heures organisées en quatre parties séquentielles. Chaque partie se décline en sous-sections : six pour la Partie 1, trois pour la Partie 2 (la deuxième sous-section couvrant sept compétences détaillées et la troisième six compétences), trois pour la Partie 3 et trois pour la Partie 4. Au total, quinze sous-sections principales structurent l'enseignement.

Les sections 5.2 et 5.3 du présent guide proposent, pour chacune de ces quinze sous-sections, d'une part les références pédagogiques recommandées (5.2) et d'autre part une proposition de démarche pédagogique en classe (5.3) comportant un schéma pédagogique séquencé et un cas pratique calibré sur le format des épreuves DSCG.

Chapitre 1 LES REFERENCES PEDAGOGIQUES POUR L'ENSEIGNANT

Cette section regroupe, pour chacune des quinze sous-sections du programme, une sélection de six à huit références pédagogiques (manuels, articles académiques, MOOC, rapports institutionnels) directement exploitables par l'enseignant. Les ouvrages de référence, notamment Laudon et Laudon (Pearson) ; Reix, Fallery, Kalika, Richet et Rowe (Vuibert) ; le manuel DSCG 5 chez Dunod ; ainsi que le DAMA-DMBOK — ont été privilégiés, de même que les publications du CIGREF (cigref.fr/publications), de l'ANSSI (cyber.gouv.fr) et de la CNIL. Il est à noter, sans qu'on le rappelle pour chaque sous-section, que les ouvrages de l'ancienne mouture du programme

et les cas qu'ils proposent constituent en eux-mêmes une source utile, tant pour les chapitres théoriques que pour les cas exploitables.

1. Analyser le rôle du SI dans l'organisation (24h)

1.1. Élaborer et aligner la stratégie des SI (4h)

[1] DSCG 5 - Management des systèmes d'information (3e éd.) — Bilet, Felidj, Liottier *(Dunod, 2023)*

https://www.dunod.com/prepas-concours/dscg-5-management-systemes-d-information-manuel-0

Manuel de référence UE5 : alignement stratégique, schéma directeur SI, modèle SAM, IT Balanced Scorecard, cas corrigés

[2] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitres 3 et 13 : alignement stratégique SI, schéma directeur, création de valeur, gouvernance. Référence internationale incontournable

[3] Évaluer le retour sur investissement des solutions d'IA générative et agentique — CIGREF, 2024 *(cigref.fr)*

https://www.cigref.fr/evaluer-le-retour-sur-investissement-des-solutions-dia-generative-et-agentique

Publication CIGREF sur l'évaluation du ROI des SI, intelligence artificielle et valeur stratégique. Très orienté terrain

[4] Strategic Alignment Model (SAM) — Henderson & Venkatraman, MIT *(JSTOR)*

https://doi.org/10.1147/sj.382.0472

Article fondateur du modèle d'alignement stratégique SI/métier. Indispensable pour les enseignants souhaitant ancrer le cours dans la théorie

[5] IT Balanced Scorecard — Van Grembergen & De Haes *(ISACA, 2005)*

Linking the IT Balanced Scorecard to the Business Objectives at a Major Canadian Financial group

Mise en lien IT BSC et objectifs métiers. Outil pédagogique central pour comprendre comment piloter l'alignement par les indicateurs

[6] Transformation numérique — cas MAIF, Décathlon, SNCF — CIGREF / Presse spécialisée *(cigref.fr)*

https://www.cigref.fr/publications

Études de cas documentées d'entreprises françaises ayant aligné ou désaligné leur SI avec leur stratégie. Supports directs pour les TD

1.2. Concevoir et piloter la gouvernance des SI (4h)

[1] Pour une meilleure gouvernance des SI — D. Moisand & F. Garnier de Labareyre *(Eyrolles, 2019)*

https://www.eyrolles.com/Informatique/Livre/cobit-9782212126280/

Ouvrage de référence francophone sur la gouvernance des SI : COBIT, ISO 38500, rôle de la DSI, tableau de bord de gouvernance, cas pratiques

[2] Modèle de maturité et d'audit de la gouvernance du numérique — CIGREF, 2023 *(cigref.fr)*

https://www.cigref.fr/modele-de-maturite-et-daudit-de-la-gouvernance-du-numerique-le-nouveau-referentiel-pour-piloter-la-maturite-de-votre-gouvernance-numerique

Référentiel CIGREF pour évaluer la maturité de la gouvernance numérique : 5 niveaux, indicateurs, grille d'audit. Directement exploitable en TD

[3] COBIT 2019 — Framework — ISACA *(isaca.org)*

https://www.isaca.org/resources/cobit

Référentiel international de gouvernance et de management des SI. Objectifs de gouvernance, processus, indicateurs. Gratuit en version de base

[4] ISO 38500 : Gouvernance des TI pour l'organisation — ISO *(iso.org)*

https://www.iso.org/fr/standard/81684.html

Norme internationale : 6 principes de gouvernance des TI (responsabilité, stratégie, acquisition, performance, conformité, comportement humain). Référence normative incontournable

[5] MOOC Gouvernance des SI — Université Paris Dauphine *(FUN MOOC)*

https://www.fun-mooc.fr/fr/cours/?search=gouvernance+systemes+information

MOOC en français sur la gouvernance SI : rôles DSI/DG/métiers, tableaux de bord, maturité numérique, indicateurs ESG. Accès libre, certifiant

1.3. Diagnostiquer et piloter l'évolution des architectures et de l'urbanisation des SI (4h)

[1] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitres 13 et 14 : cartographie applicative, architectures SI, urbanisation, EAI/API, processus et intégration. Référence pédagogique de base

[2] BPMN 2.0 — Guide de référence — OMG / Processmaker *(omg.org)*

https://www.omg.org/spec/BPMN/2.0/

Standard international de modélisation des processus métiers. Indispensable pour la cartographie des processus et l'analyse des flux SI/métier

[3] ArchiMate 3.2 — Documentation officielle — The Open Group *(opengroup.org)*

The ArchiMate® Enterprise Architecture Modeling Language | www.opengroup.org

Langage de modélisation d'architecture d'entreprise : couches métier, applicative et technologique. Outil de référence pour la cartographie SI

[4] Intelligence artificielle : guide à destination des dirigeants — CIGREF / BCG, 2023 *(cigref.fr)*

https://www.cigref.fr/guide-de-mise-en-oeuvre-de-lai-act-mode-demploi-et-outils-pour-mettre-en-place-une-gouvernance-de-lia

Panorama des IA et de leur impact sur les architectures SI, les processus métiers et les modèles d'affaires. Cas d'usage concrets, niveau DSCG

[5] Blockchain for Good Research — The Blockchain for Good Research, 2023 *(research.theblockchainforgood.org)*

https://research.theblockchainforgood.org

Recherches sur les usages de la blockchain dans les organisations : traçabilité, audit, smart contracts, gouvernance. Cas sectoriels documentés

[6] Panorama Process Mining — Gartner / Celonis Academy, 2024 *(celonis.com)*

https://academy.celonis.com/

Introduction au Process Mining : analyse des flux de données réels issus des ERP, identification des anomalies de processus, outil pédagogique adapté

1.4. Gérer les relations contractuelles et opérationnelles avec les ESN (4h)

[1] DSCG 5 - Management des systèmes d'information (3e éd.) — Bilet, Felidj, Liottier *(Dunod, 2023)*

https://www.dunod.com/prepas-concours/dscg-5-management-systemes-d-information-manuel-0

Manuel de référence UE5 : contrats ESN, SLA, infogérance, clauses de réversibilité, pilotage des prestataires SI. Cas corrigés

[2] Guide de l'infogérance & SLA— IBM

https://www.ibm.com/fr-fr/think/topics/service-level-agreement

Guide IBM : typologies de prestations ESN, contenu des SLA, indicateurs de performance, clauses essentielles (réversibilité, propriété intellectuelle, RGPD)

[3] Le contrat informatique — J. Huet & E. Dreyer *(LGDJ, 2022)*

https://www.lgdj.fr/droit-de-la-communication-numerique-9782275034904.html

Référence juridique sur les contrats informatiques : obligations de résultat/moyens, propriété intellectuelle, responsabilité, clauses de confidentialité et de sécurité

[4] ITIL 4 — Foundation Guide — AXELOS, 2019 *(axelos.com)*

https://www.axelos.com/certifications/itil-service-management/itil-4-foundation

Référentiel de gestion des services SI : SLA, OLA, catalogue de services, gestion des incidents. Base pour comprendre les engagements contractuels avec les ESN.

[5] Réversibilité dans les contrats cloud — CIGREF, 2020 *(cigref.fr)*

https://www.cigref.fr/le-cigref-publie-son-referentiel-du-cloud-de-confiance

Publication CIGREF sur la réversibilité, portabilité et interopérabilité dans les contrats cloud : enjeux juridiques, clauses recommandées, risques de vendor lock-in.

[6] Marchés publics de prestations informatiques — DAE / Direction des Achats de l'État, 2023 *(economie.gouv.fr)*

https://www.economie.gouv.fr/dae/la-fonction-achat/systeme-dinformation-achat

Guide des marchés publics de SI : expression du besoin, cahier des charges, procédures d'appel d'offres, critères de sélection. Pertinent pour les entités publiques.

1.5. Planifier, organiser et conduire des projets de systèmes d'information (4h)

[1] Management d'un Projet Systèmes d'information, 8e éd. — C. Morley *(Dunod, 2022)*

https://www.dunod.com/sciences-techniques/management-d-un-projet-systeme-d-information-principes-techniques-mise-en-0

Ouvrage de référence sur la gestion de projet SI : cycle en V, méthodes agiles, MOA/MOE, RACI, gestion des risques, qualité, plan de tests. Cas pratiques intégrés.

[2] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitre 14 : gestion de projet SI, facteurs de succès et d'échec, méthodes classiques et agiles, outils de pilotage.

[3] Guide PMBOK 7e éd. — PMI (Project Management Institute), 2021 *(pmi.org)*

https://www.pmi.org/standards/pmbok

Référentiel international de gestion de projet : principes, domaines de performance, outils, planification, risques, qualité. Base théorique incontournable.

[4] Scrum Guide (version officielle en français) — K. Schwaber & J. Sutherland, 2020 *(scrumguides.org)*

https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-French.pdf

Guide officiel Scrum en français : rôles (PO, SM, équipe), artefacts (backlog, sprint), cérémonies. Référence pour la compréhension des méthodes agiles.

[5] Rapport Chaos — Bilan des projets informatiques — Standish Group, 2020 *(standishgroup.com)*

https://www.standishgroup.com

Statistiques mondiales sur les taux de succès et d'échec des projets SI : facteurs de réussite, dépassements budgétaires, causes d'abandon. Données chiffrées exploitables en cours.

[6] AMDEC appliquée aux projets SI — Référentiel AFNOR (NF EN 60812) — AFNOR *(boutique.afnor.org)*

https://www.boutique.afnor.org/fr-fr/norme/nf-en-iec-60812/analyse-des-modes-de-defaillance-et-de-leurs-effets-amde-et-amdec/fa190819/82106

Méthode AMDEC adaptée aux projets SI : identification des modes de défaillance, criticité, plan de mitigation. Outil pratique de gestion des risques projet.

1.6. Mettre en œuvre et piloter la gestion des connaissances au sein du SI (4h)

[1] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitre 11 : Knowledge Management, systèmes de gestion des connaissances, GED, systèmes experts, rôle des SI dans la capitalisation organisationnelle.

[2] La gestion des connaissances (Knowledge Management) — I. Nonaka & H. Takeuchi *(Cairn (synthèse The Knowledge-Creating Company))*

https://www.eyrolles.com/Entreprise/Livre/la-connaissance-creatrice-9782744500343/

Ouvrage fondateur du KM : modèle SECI (Socialisation, Externalisation, Combinaison, Internalisation), connaissances tacites vs explicites. Base théorique indispensable.

[3] MOOC Gestion documentaire et gouvernance des données — Université de Rennes *(FUN MOOC, 2024)*

https://www.fun-mooc.fr/fr/cours/de-la-gestion-documentaire-a-la-gouvernance-des-donnees/

20h, gratuit — GED, Records Management, gouvernance des connaissances, IA générative et recherche documentaire. Directement applicable à la section 1.6.

[4] SharePoint et la gestion des connaissances en entreprise — Microsoft Learn, 2024 *(learn.microsoft.com)*

https://learn.microsoft.com/fr-fr/sharepoint/introduction

Plateforme collaborative incontournable : gestion documentaire, wikis, bases de connaissances, flux collaboratifs. Cas d'usage entreprise.

[5] IA générative et gestion des connaissances : enjeux et opportunités — CIGREF, 2023 *(cigref.fr)*

https://www.cigref.fr/innovations-technologiques-enjeux-et-opportunites-pour-les-systemes-dinformation

Impact de l'IA générative sur le KM : synthèse automatique, moteurs de recherche sémantique, assistants cognitifs. Opportunités et risques (hallucinations, confidentialité).

[6] Records Management et archivage électronique — AAF / Archives de France, 2020 *(archivesdefrance.culture.gouv.fr)*

https://vsa-aas.ch/fr/association/groupes-de-travail/records-management-et-archivage-electronique/

Normes et bonnes pratiques de Records Management (ISO 15489) : cycle de vie documentaire, archivage électronique, durées de conservation légales. Perspective juridique et organisationnelle.

2. Organiser, exploiter et sécuriser les données de l'organisation (48h)

2.1. Concevoir l'organisation des données et assurer leur interopérabilité (4 heures)

[1] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Manuel international de référence (chapitre 6 sur les fondations de la BI : entrepôts de données, Big Data, gestion des données). Ouvrage cité dans la trame officielle DSCG.

[2] DAMA-DMBOK : Data Management Body of Knowledge (2e édition) — DAMA International *(Technics Publications, 2017)*

https://www.dama.org/cpages/body-of-knowledge

Référentiel international de la gestion des données (11 domaines de connaissance). Source mentionnée dans la trame officielle DSCG.

[3] DSCG 5 — Management des systèmes d'information (manuel et applications) — F. Bilet et al. *(Dunod Expert Sup, 2024)*

https://www.dunod.com/prepas-concours/dscg-5-management-systemes-d-information-manuel-0

Manuel pédagogique conçu spécifiquement pour le DSCG : modélisation conceptuelle (MCD/MLD), interopérabilité, formats d'échange. Cas et corrigés calibrés examen.

[4] Bases de données relationnelles : apprendre pour utiliser (MOOC) — FUN MOOC / INRIA *(FUN MOOC, 2024)*

https://www.fun-mooc.fr/fr/cours/?search=bases+de+donnees+relationnelles

MOOC certifiant : modélisation, SQL, normalisation. 6 semaines, accès libre. Excellente remise à niveau pour les étudiants non issus de filières techniques.

[5] Data Lake vs Data Warehouse : différences — Datagalaxy *(Datagalaxy Blog, 2025)*

https://www.datagalaxy.com/fr/blog/data-lake-vs-data-warehouse-differences/

Comparatif structuré des architectures de données : usages, gouvernance, coûts. Support de TD pour comprendre les choix d'architecture.

[6] Fichier des écritures comptables (FEC) — Format standard — DGFiP *(impots.gouv.fr, 2024)*

https://www.impots.gouv.fr/fichiers-standards-des-ecritures-comptables

Norme officielle française d'interopérabilité comptable : structure du FEC, formats, contrôles fiscaux. Référence légale incontournable pour les experts-comptables.

[7] Réversibilité, portabilité et interopérabilité dans les contrats cloud — CIGREF *(cigref.fr, 2023)*

https://www.cigref.fr/le-cigref-publie-son-referentiel-du-cloud-de-confiance

Publication CIGREF dédiée à l'interopérabilité contractuelle des données dans les services cloud : clauses-types, audits, indicateurs.

[8] Le monde de l'Internet des objets (rapport) — France Stratégie *(strategie.gouv.fr, 2022)*

https://www.strategie-plan.gouv.fr/files/files/Publications/2021%20SP/2022-02-17%20-%20Le%20monde%20de%20l%27internet%20des%20objets/fs-2022-rapport-iot-fevrier.pdf

Rapport public approfondi sur l'IoT : volumétrie de données, interopérabilité, défis de gouvernance. Source institutionnelle française pour élargir la perspective.

2.2. Collecter, traiter, analyser et interpréter des données à des fins décisionnelles (28h)

[1] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitre 12 sur l'aide à la décision (BI, analytics, data mining, IA, dashboards). Ouvrage cité dans la trame officielle DSCG.

[2] DAMA-DMBOK : Data Management Body of Knowledge (2e édition) — DAMA International *(Technics Publications, 2017)*

https://www.dama.org/cpages/body-of-knowledge

Domaines spécifiques : Data Quality, Data Integration, Business Intelligence and Analytics, Reference and Master Data. Référentiel cité dans la trame officielle.

[3] Réalisez des dashboards avec Power BI (cours certifiant) — OpenClassrooms *(OpenClassrooms, 2025)*

https://openclassrooms.com/fr/courses/7110891-realisez-des-dashboards-avec-power-bi

8h, accès libre — Power Query, modèle relationnel, visualisations, publication. Complément TP idéal au manuel Bilet/Dunod.

[4] TCD et outils d'aide à la décision Excel (documentation officielle) — Microsoft Support *(Microsoft Support, 2024)*

https://support.microsoft.com/fr-fr/office/utiliser-les-tableaux-crois%C3%A9s-dynamiques-et-les-autres-outils-d-aide-%C3%A0-la-d%C3%A9cision-pour-analyser-vos-donn%C3%A9es-da1b3e85-d3c0-4f15-8cd9-bef446762ec3

Documentation officielle complète : TCD, Power Pivot, chronologies, DAX. Support technique fiable pour les TD.

[5] Atteindre ses objectifs avec le tableau de bord prospectif (Balanced Scorecard) — Hub.brussels *(Hub.brussels, 2025)*

http://info.hub.brussels/guide/gestion-strategies/affinez-votre-strategie-laide-dun-tableau-de-bord-prospectif

Balanced Scorecard complet : 4 axes, carte stratégique, KPI SMART, indicateurs ESG. Pédagogie progressive.

[6] Les biais cognitifs : comment nous nous trompons (présentation institutionnelle) — CEREMA *(CEREMA, 2019)*

https://www.cerema.fr/system/files/documents/2019/11/bocquet_m-050519_presentation_cotita_biais_cognitifs_v3.pdf

Corrélation vs causalité, biais de confirmation, ancrage, extrapolation. Référence institutionnelle pour la phase d'interprétation des résultats.

[7] Décisions d'investissement (cours universitaire VAN/TRI) — AUNEGE — Université Numérique *(moodle.luniversitenumerique.fr, 2024)*

https://moodle.luniversitenumerique.fr/pluginfile.php/4241/mod_resource/content/0/Lecon_5_AUNEGE_La_politique_dinvestissement.pdf

Cours académique en accès libre : VAN, TRI, choix entre projets, arbres de décision. Référentiel AUNEGE des universités numériques.

[8] Évaluer le retour sur investissement des solutions d'IA générative et agentique — CIGREF *(cigref.fr, 2025)*

https://www.cigref.fr/evaluer-le-retour-sur-investissement-des-solutions-dia-generative-et-agentique

Publication CIGREF dédiée à la mesure du ROI des solutions d'IA : indicateurs financiers et non financiers, méthodologie, retours d'expérience.

2.3. Elaborer et piloter la gouvernance stratégique des données *(16 heures)*

[1] Management des Systèmes d'information, 18e éd. — K. Laudon & J. Laudon *(Pearson, 2026)*

https://www.pearson.fr/fr/book/?gcoi=27440100439730

Chapitre 6 sur la gestion des données et la gouvernance. Ouvrage cité dans la trame officielle DSCG.

[2] Guide de la sécurité des données personnelles — CNIL *(cnil.fr, 2024)*

https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_des_donnees_personnelles-2023.pdf

Guide officiel de la CNIL : cycle de vie matériels/logiciels, traçabilité, gestion des incidents, notification, registre des traitements. Référence incontournable RGPD.

[3] Le règlement sur les données (Data Act) — cadre européen — CNIL *(cnil.fr, 2025)*

https://www.cnil.fr/fr/reglement-donnees-data-act-nouveau-cadre-europeen-pour-partage-utilisation-donnees

Data Act européen (en application depuis sept. 2025) : accès aux données IoT, obligations des fabricants, articulation avec RGPD et DGA.

[4] Cloud Computing — État de la menace informatique — ANSSI / CERT-FR *(cyber.gouv.fr, 2025)*

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-001.pdf

Rapport ANSSI de 46 pages : menaces cloud (IaaS/PaaS/SaaS), mauvaises configurations, attaques ciblant fournisseurs et clients. Données récentes exploitables en TD.

[5] ISO/IEC 27001:2022 — Sécurité de l'information (fiche officielle) — Organisation internationale de normalisation *(iso.org, 2022)*

https://www.iso.org/fr/standard/27001

Fiche officielle de la norme : champ d'application, exigences SMSI (CIA), structure normative, articulation avec ISO 27002. Référence pour les audits.

[6] Comptabilité des crypto-actifs — règlement ANC 2020-05 — CryptoAccounting.fr *(cryptoaccounting.fr, 2025)*

https://cryptoaccounting.fr/blog/le-reglement-anc-n-2020-05-decrypte-comptabilite-des-crypto-actifs-des-entreprises-francaises

Décryptage du règlement ANC 2020-05 : comptes 521/522, ICO, staking, plus-values CMUP/FIFO. Très ciblé expertise comptable.

[7] Les crypto-actifs : une régulation à renforcer (rapport) — Cour des comptes *(ccomptes.fr, 2023)*

https://www.ccomptes.fr/sites/default/files/2023-12/S2023_1247_Crypto_actifs.pdf

Rapport officiel : définition juridique, fiscalité DGFiP, PSAN (loi PACTE), règlement MiCA, lutte anti-blanchiment. Source de référence française.

[8] Monétisation des données personnelles — Combien valent nos données ? — CNIL *(cnil.fr, 2025)*

https://www.cnil.fr/fr/monetisation-des-donnees-personnelles-combien-valent-nos-donnees

Approche économique et juridique de la monétisation des données : valeur marchande, limites RGPD, enjeux éthiques. Pédagogique et structuré.

3. Mettre en œuvre les outils SI au service de la performance organisationnelle (32h)

3.1. Concevoir, construire et exploiter des outils de pilotage de la performance (12h)

[1] DSCG 5 - Management des systèmes d'information (3e éd.) — Bilet, Felidj, Liottier *(Dunod, 2023)*

https://www.dunod.com/prepas-concours/dscg-5-management-systemes-d-information-manuel-0

Manuel de référence UE5 — chapitres consacrés au contrôle de gestion SI, TCO, indicateurs de performance et tableaux de bord. Cas corrigés directement réutilisables.

[2] Modèle d'analyse de la valeur du SI — Référentiel CIGREF — CIGREF, 2022 *(cigref.fr)*

https://www.cigref.fr/rapport-cigref-valeur-economique-projet-transformation-numerique-entreprise-approche-methodologique

Cadre méthodologique français pour évaluer la contribution du SI à la création de valeur : indicateurs de performance, alignement stratégique, ROI numérique. Très ancré dans la pratique des DSI françaises.

[3] COBIT 2019 — Performance Management Guide — ISACA *(isaca.org)*

https://www.isaca.org/resources/cobit

Référentiel international de management de la performance SI : objectifs de gouvernance, indicateurs, niveaux de capacité. Module gratuit en téléchargement après inscription.

[4] Méthode ABC (Activity-Based Costing) appliquée aux SI — P. Mévellec / J.-L. Malo *(Revue française de gestion)*

https://www.cairn.info/revue-francaise-de-gestion.htm

Articles méthodologiques sur la comptabilité par activités appliquée aux fonctions support. Fondamental pour comprendre l'analyse des coûts cachés et indirects de la fonction SI.

[5] ITIL 4 — Service Value System — AXELOS / PeopleCert, 2019 *(axelos.com)*

https://www.axelos.com/certifications/itil-service-management

Référentiel ITIL 4 : pratiques de gestion des services SI, mesure de la valeur, indicateurs de performance opérationnelle. Chapitres « Continual Improvement » et « Measurement and Reporting » pertinents pour le DSCG.

[6] Construire un tableau de bord SI — Guide pratique CIGREF — CIGREF, 2021 *(cigref.fr)*

https://www.cigref.fr/publications

Méthodologie de construction d'un tableau de bord SI orienté pilotage stratégique : choix des KPI, hiérarchisation, intégration des indicateurs ESG et de cybersécurité. Ressource opérationnelle.

3.2. Auditer, contrôler et évaluer la performance et la conformité des SI (12h)

[1] DSCG 5 – Management des systèmes d'information (3e éd.) — Bilet, Felidj, Liottier *(Dunod, 2023)*

https://www.dunod.com/prepas-concours/dscg-5-management-systemes-d-information-manuel-0

Manuel de référence UE5 — partie consacrée à l'audit SI : démarche, normes NEP applicables, articulation avec l'audit financier. Cas corrigés.

[2] NEP 315 — Connaissance de l'entité et de son environnement, dont le contrôle interne — CNCC / H3C *(h3c.org)*

https://h2a-france.org/normes/connaissance-de-lentite-et-de-son-environnement-et-evaluation-du-risque-danomalies-significatives-dans-les-comptes/

Norme d'exercice professionnel structurante pour l'audit SI dans une mission de commissariat aux comptes : évaluation du contrôle interne automatisé, identification des risques liés aux SI, conséquences sur la stratégie d'audit.

[3] COBIT 2019 — Framework: Governance and Management Objectives — ISACA *(isaca.org)*

https://www.isaca.org/resources/cobit

Référentiel international d'audit SI : 40 objectifs de gouvernance et de management, indicateurs de capacité (CMMI 0-5), processus d'audit. Base structurante des missions d'audit SI.

[4] ISO/IEC 27001:2022 — SMSI et audit de conformité — ISO / AFNOR *(iso.org)*

https://www.iso.org/fr/standard/27001

Norme internationale de référence pour l'audit du système de management de la sécurité de l'information (SMSI) : exigences, contrôles, processus de certification. Indispensable pour situer un audit SI dans un cadre normatif reconnu.

3.3. Appréhender les usages et les enjeux des technologies de la blockchain et des cryptoactifs (8h)

[1] Les crypto-actifs : une régulation à renforcer — Cour des comptes, 2023 *(ccomptes.fr)*

https://www.ccomptes.fr/sites/default/files/2023-12/S2023_1247_Crypto_actifs.pdf

Rapport public officiel : définition juridique des cryptoactifs, fiscalité DGFiP, statut PSAN (loi PACTE), articulation avec MiCA, lutte anti-blanchiment. Source institutionnelle de référence pour aborder le cadre réglementaire.

[2] Règlement MiCA — Markets in Crypto-Assets (UE 2023/1114) — Union européenne *(EUR-Lex)*

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32023R1114

Texte officiel du règlement européen MiCA, applicable depuis décembre 2024 : statuts ART/EMT, obligations des émetteurs et prestataires de services, articulation avec la directive DAC8. Indispensable pour le volet réglementaire.

[3] Règlements ANC 2020-05 et 2026-02 — Comptabilité des cryptoactifs — Autorité des normes comptables *(anc.gouv.fr)*

https://www.anc.gouv.fr/normes-comptables-francaises/reglements-de-lanc

Cadre comptable français des cryptoactifs : ANC 2020-05 (entreprises commerciales) et ANC 2026-02 (établissements bancaires, cadre MiCA). Comptes 521/522, méthodes CMUP/FIFO, traitement des plus-values. Très ciblé profession comptable.

[4] Rapport Les enjeux des blockchains - Haut Commissariat à la stratégie et au plan

https://www.strategie-plan.gouv.fr/publications/enjeux-blockchains

Rapport officiel France Stratégie : usages de la blockchain dans les organisations (audit, traçabilité, contrats intelligents), enjeux de gouvernance, cas sectoriels documentés. Ressource pédagogique francophone solide.

[5] Transformation de la comptabilité avec la Blockchain (article académique) — Cairn — Revue ACCRA *(shs.cairn.info, 2019)*

https://shs.cairn.info/revue-accra-2019-2-page-5?lang=fr

Article académique en accès libre dans la Revue ACCRA (Audit, Comptabilité, Contrôle : Recherches Appliquées) : implications de la blockchain pour la profession comptable, transformation des métiers, piste d'audit fiable. Référence citée dans la trame officielle DSCG.

[6] Comprendre la blockchain (dossier pédagogique) — La Finance pour Tous — IEFP *(lafinancepourtous.com, 2024)*

https://www.lafinancepourtous.com/decryptages/finance-et-societe/nouvelles-economies/blockchain/quest-ce-que-la-blockchain/

Dossier pédagogique grand public de l'Institut pour l'Éducation Financière du Public (IEFP) : fondamentaux de la blockchain, illustrations, glossaire. Ressource d'introduction citée dans la trame officielle DSCG.

[7] Les enjeux technologiques des blockchains (rapport parlementaire) — OPECST — Sénat *(senat.fr, 2018)*

https://www.senat.fr/rap/r17-584/r17-58434.html

Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques : panorama exhaustif blockchain, enjeux pour les services financiers, recommandations institutionnelles. Référence citée dans la trame officielle DSCG.

4. Sécuriser et rendre durable le système d'information (36h)

4.1. Identifier, analyser et gérer les risques liés aux systèmes d'information (12h)

[1] EBIOS Risk Manager — Méthode officielle d'analyse de risques cyber — ANSSI, 2018 (mises à jour régulières) *(ssi.gouv.fr)*

https://cyber.gouv.fr/securisation/analyse-des-risques/methode-ebios-rm/

Méthode française de référence pour l'analyse des risques cyber, structurée en 5 ateliers. Documents officiels gratuits, exemples sectoriels, fiches méthodologiques. Pierre angulaire de la formation au risque SI en France.

[2] Panorama de la cybermenace 2025 — ANSSI / CERT-FR *(cyber.gouv.fr, mars 2026)*

https://cyber.gouv.fr/nous-connaitre/publications/panoramas-de-la-cybermenace/panorama-de-la-cybermenace-2025/

Rapport annuel officiel sur l'état de la menace cyber en France : 1 366 incidents traités en 2025, exfiltration de données en hausse de 51 %, secteurs les plus visés (éducation 34 %, ministères 24 %, santé 10 %), évolution des techniques. Données chiffrées exploitables directement en cours.

[3] MEHARI — Méthode d'analyse et de management des risques — CLUSIF *(clusif.fr)*

https://clusif.fr/services/management-des-risques/les-versions-de-mehari/

Méthode francophone alternative à EBIOS, particulièrement adaptée aux PME : grille d'évaluation des vulnérabilités, base de connaissances de 200 services de sécurité, ressources gratuites pour la formation.

[4] ISO 31000:2018 et ISO 27005:2022 — Management des risques — ISO / AFNOR *(iso.org)*

https://www.iso.org/fr/standard/65694.html

Cadres normatifs internationaux : ISO 31000 (management des risques en général) et ISO 27005 (risques liés à la sécurité de l'information). Vision systémique du risque, articulation avec ISO 27001.

[5] NEP 240, 260 et 315 — Risques et systèmes d'information dans l'audit — CNCC / H3C *(h3c.org)*

https://h2a-france.org/normes/connaissance-de-lentite-et-de-son-environnement-et-evaluation-du-risque-danomalies-significatives-dans-les-comptes/

Normes d'exercice professionnel structurantes : NEP 240 (fraude, dont fraude SI), NEP 260 (communication avec les organes de gouvernance) et NEP 315 (risques SI dans l'évaluation du contrôle interne). Indispensables pour le volet audit.

[6] Guide CNIL — Sécurité des données personnelles (édition 2024) — CNIL *(cnil.fr)*

https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles

25 fiches thématiques opérationnelles : authentification, sauvegardes, sous-traitance, cloud, IA. Croisement risque cyber et risque réglementaire RGPD. Référence officielle gratuite.

4.2. Concevoir, mettre en œuvre et contrôler une politique de sécurité des SI (14h)

[1] Guide d'hygiène informatique (édition 2024) — ANSSI *(cyber.gouv.fr)*

https://cyber.gouv.fr/publications/guide-dhygiene-informatique

42 mesures de sécurité essentielles classées en 9 thèmes : sensibilisation, gestion des accès, sécurisation des postes, sauvegardes, supervision. Référence officielle française incontournable pour la PSSI.

[2] ISO/IEC 27001:2022 — Système de management de la sécurité de l'information — ISO / AFNOR *(iso.org)*

https://www.iso.org/fr/standard/27001

Norme internationale de référence pour le SMSI : 93 mesures de sécurité (Annexe A), processus de certification, articulation avec ISO 27002 (guide d'application). Cadre normatif central de toute politique de sécurité SI.

[3] Directive NIS 2 (UE 2022/2555) et règlement DORA (UE 2022/2554) — Union européenne *(EUR-Lex)*

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555

Cadres réglementaires européens applicables depuis 2024-2025 : NIS2 (entités essentielles et importantes), DORA (résilience opérationnelle numérique du secteur financier). Obligations de gouvernance, gestion des risques, signalement d'incidents.

[4] ISO 31000:2018 — Management du risque (lignes directrices) — Organisation internationale de normalisation *(iso.org, 2018)*

https://www.iso.org/fr/standard/65694.html

Norme internationale de référence pour le management du risque : principes, cadre organisationnel, processus. Articulée avec ISO 27001 et ISO 27005 pour la dimension cyber. Référence citée dans la trame officielle DSCG.

[5] SecNumacademie — MOOC officiel de l'ANSSI — ANSSI *(messervices.cyber.gouv.fr)*

https://messervices.cyber.gouv.fr/services/secnum-academie.html

MOOC certifiant gratuit en français : 4 modules (panorama SSI, sécurisation du poste, authentification, internet et nomadisme). Ressource pédagogique adaptée au niveau DSCG.

[6] Guide PCA/PRA — Plan de continuité d'activité — SGDSN / ANSSI *(sgdsn.gouv.fr)*

https://infolettre.developpement-durable.gouv.fr/IMG/pdf/guide_methodologique_elaboration_pca_pra_cyber-2.pdf

Guide officiel français sur l'élaboration d'un PCA/PRA : méthodologie, contenus types, tests, gouvernance. Indispensable pour le volet résilience et continuité opérationnelle.

4.3. Intégrer les enjeux de durabilité et de sobriété numérique dans le management des SI (10h)

[1] Directive CSRD et normes ESRS — Reporting de durabilité — EFRAG / ANC *(efrag.org)*

https://www.efrag.org/en/sustainability-reporting/esrs-workstreams

Documentation officielle de la directive CSRD (UE 2022/2464) et des 12 normes ESRS publiées en juillet 2023. Architecture, périmètre, double matérialité, indicateurs spécifiques. Source de référence pour le volet reporting durabilité.

[2] Référentiel général d'écoconception des services numériques (RGESN) — DINUM / ARCEP / ADEME

*(ecoresponsable.numerique.gouv.fr)*https://ecoresponsable.numerique.gouv.fr/publications/referentiel-general-ecoconception/

Référentiel officiel français d'écoconception des services numériques (78 critères en version 2024) : sobriété, accessibilité, durabilité matérielle. Outil opérationnel directement exploitable.

[3] Loi REEN (Réduire l'Empreinte Environnementale du Numérique) du 15 novembre 2021 — République française *(Légifrance)*

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044327272

Texte législatif structurant l'engagement français en matière de numérique responsable : sensibilisation, durabilité matérielle, écoconception, datacenters. Articulation avec la stratégie nationale Numérique Responsable.

[4] Stratégies Numérique Responsable des grandes organisations : comment passer à l'échelle ? — CIGREF *(cigref.fr, 2025)*

https://www.cigref.fr/strategies-numerique-responsable-des-grandes-organisations-comment-passer-a-lechelle

Publication CIGREF de référence : leviers stratégiques, gouvernance du numérique responsable, indicateurs, retours d'expérience de grandes organisations. Référence citée dans la trame officielle DSCG.

[5] EcoIndex et GreenIT Analysis — Outils de mesure d'empreinte numérique — Collectif GreenIT.fr / ADEME *(ecoindex.fr)*

https://www.ecoindex.fr

Outils gratuits et ouverts d'évaluation de la performance environnementale des sites web et services numériques. Méthode reconnue, exploitable en TD pour mesurer concrètement l'empreinte d'applications réelles.

[6] L'approche low-tech au service de la résilience numérique des organisations — CIGREF / Institut du Numérique Responsable *(cigref.fr, 2025)*

https://www.cigref.fr/lapproche-low-tech-au-service-de-la-resilience-numerique-des-organisations-strategies-dadaptation-face-aux-fluctuations

Rapport CIGREF/INR sur la sobriété numérique appliquée : stratégies d'adaptation face aux fluctuations énergétiques et géopolitiques, principes low-tech, bonnes pratiques. Référence citée dans la trame officielle DSCG.

Chapitre 2 PROPOSITIONS DE DEMARCHE PEDAGOGIQUE EN CLASSE

Cette section propose, pour chacune des quinze sous-sections du programme, une démarche pédagogique structurée comportant :

- un schéma pédagogique séquencé en plusieurs phases (cours magistral, travaux dirigés, travaux pratiques) avec durées indicatives à adapter au format de formation retenu ;
- un cas pratique type DSCG inspiré d'organisations réalistes, calibré sur le format des épreuves d'examen, comportant un contexte, cinq questions de difficulté graduée et des annexes documentaires à élaborer.

L'ensemble des cas pratiques mobilise les références listées en section 5.2 et propose, pour chaque sous-section, des situations professionnelles directement transposables en salle.

1. Analyser le rôle du SI dans l'organisation (48h)

1.1. Élaborer et aligner la stratégie des SI (12h)

- **Schéma pédagogique proposé**

Phase 1 (4h) : Cours magistral — Définition et enjeux de l'alignement stratégique SI/métier ; modèle SAM (Henderson & Venkatraman) ; IT Balanced Scorecard ; rôle du schéma directeur des SI ; indicateurs d'évaluation de l'alignement ; intégration des critères ESG.

Phase 2 (3h) : TD analyse de cas — Étude comparative de 2 entreprises (cas MAIF ou Décathlon vs cas d'échec type LOUVOIS ou FoxMeyerDrug) : identifier les facteurs d'alignement ou de désalignement stratégique SI/métier. Grille d'analyse structurée. Restitution en binômes.

Phase 3 (5h) : Cas pratique — À partir d'un extrait de rapport annuel ou de schéma directeur, évaluer le niveau d'alignement stratégique d'une organisation, proposer des axes d'amélioration et formuler des recommandations orientées création de valeur et RSE.

- **Cas pratique type DSCG**

Le groupe HORIZONS SERVICES — Évaluation de l'alignement stratégique SI/métier

Contexte : HORIZONS SERVICES est un groupe de services à la personne (CA 120 M€, 8 filiales, 1 800 salariés) dont la stratégie de croissance repose sur la différenciation par la qualité de la relation client et l'innovation dans les services digitaux. À la suite d'une fusion-acquisition, le groupe dispose de 3 SI hétérogènes (CRM différents, ERP non interconnectés, outils de reporting disparates). La Direction Générale mandate un cabinet d'expertise comptable pour réaliser un diagnostic d'alignement stratégique SI/métier avant d'engager un programme de transformation SI sur 3 ans.

Travail demandé :

1. Analyser l'alignement stratégique entre la stratégie métier d'HORIZONS SERVICES et l'architecture SI actuelle à l'aide du modèle SAM (Henderson & Venkatraman). Identifier les zones de cohérence et les dysfonctionnements majeurs.

2. Évaluer, à partir des documents fournis en annexe, les 4 perspectives de l'IT Balanced Scorecard (performance financière, satisfaction des utilisateurs, processus internes SI, apprentissage et innovation). Proposer 2 indicateurs mesurables par perspective.

3. Proposer les axes prioritaires d'un schéma directeur SI triennal : diagnostic, vision cible, 3 axes stratégiques, indicateurs de pilotage. Justifier les arbitrages réalisés au regard des objectifs métier et des contraintes RSE du groupe.

4. Identifier les principaux risques de désalignement lors de la phase de transformation (résistances organisationnelles, hétérogénéité des SI, dépendance aux prestataires) et proposer des mesures de mitigation.

5. Formuler une recommandation sur l'intégration d'indicateurs ESG dans le pilotage du schéma directeur SI : quels indicateurs retenir, comment les articuler avec les objectifs stratégiques du groupe ?

Annexes : Annexe 1 : Extrait du plan stratégique HORIZONS SERVICES 2025-2028 — Annexe 2 : Cartographie SI actuelle (3 ERP, 3 CRM, outils de reporting) — Annexe 3 : Grille IT Balanced Scorecard (à compléter) — Annexe 4 : Tableau de bord de direction actuel (indicateurs financiers et RH uniquement) — Annexe 5 : Benchmark sectoriel services à la personne (maturité numérique).

1.2. Concevoir et piloter la gouvernance des SI (10h)

- **Schéma pédagogique proposé**

Phase 1 (2h30) : Cours magistral — Modèles organisationnels de la DSI (centralisé, décentralisé, fédéré, externalisé) ; rôles et missions de la DSI ;

relations DSI/DG/métiers ; rôles émergents (CDO, DOSI, CTO) ; référentiels COBIT, ISO 38500 ; maturité numérique (Digital Maturity Model) ; tableau de bord SI intégrant critères ESG.

Phase 2 (3h30) : TD comparatif — À partir de 3 fiches d'organisation SI (PME sous-traitante, grand groupe industriel, collectivité territoriale) : identifier le modèle organisationnel de chaque DSI, ses forces et faiblesses, et proposer des pistes d'amélioration de la gouvernance. Travail en groupes, restitution collective.

Phase 3 (4h) : Cas diagnostic — Évaluation de la maturité numérique d'une organisation à partir d'une grille CIGREF (5 niveaux de maturité, 6 dimensions) : positionnement, identification des axes de progression, construction d'un tableau de bord de gouvernance SI avec indicateurs de performance et indicateurs ESG.

- **Cas pratique type DSCG**

Le groupe CONSULT-PARTNERS — Diagnostic de gouvernance SI et maturité numérique

Contexte : CONSULT-PARTNERS est un groupe de conseil et d'expertise (250 collaborateurs, 3 entités, CA 38 M€) dont la DSI est structurée de façon décentralisée : chaque entité gère ses propres outils informatiques, avec une coordination centrale limitée à la messagerie et à la facturation. Suite à un audit interne révélant des incidents de sécurité répétés, une absence de politique de données homogène et une satisfaction utilisateur dégradée (NPS SI = –12), la Direction Générale souhaite revoir l'organisation et la gouvernance de son SI.

Travail demandé :

1. Analyser le modèle organisationnel actuel de la DSI de CONSULT-PARTNERS (annexe 1). Identifier ses avantages et ses limites au regard des enjeux de performance, de sécurité et de cohérence du groupe. Proposer un modèle alternatif adapté à la taille et au secteur de l'organisation.

2. Évaluer la maturité numérique du groupe à l'aide de la grille fournie en annexe 2 (6 dimensions : stratégie, processus, data, sécurité, compétences, culture). Positionner l'entreprise sur l'échelle de maturité CIGREF (niveaux 1 à 5) et justifier l'évaluation.

3. Concevoir un tableau de bord de gouvernance SI adapté à CONSULT-PARTNERS : sélectionner 6 KPI pertinents (2 techniques, 2 économiques, 2 ESG), préciser leur formule de calcul et leur fréquence de suivi.

4. Analyser les relations entre la DSI, la Direction Générale et les directions métiers (annexe 3). Identifier les dysfonctionnements (silos, absence de pilotage transversal, rôles non clarifiés) et proposer une cartographie des rôles cible intégrant un CDO ou un DOSI.

5. Formuler 5 recommandations priorisées pour améliorer la gouvernance SI de CONSULT-PARTNERS, en distinguant actions rapides (3 mois) et restructurations profondes (12-18 mois). Justifier la priorisation au regard des enjeux stratégiques.

Annexes : Annexe 1 : Organigramme SI actuel du groupe (3 entités, IT locaux, DSI centrale limitée) — Annexe 2 : Grille de maturité numérique CIGREF (6 dimensions, à évaluer) — Annexe 3 : Résultats de l'enquête satisfaction collaborateurs SI (extraits) — Annexe 4 : Rapport d'audit interne SI (incidents, données, conformité RGPD) — Annexe 5 : Benchmark gouvernance SI secteur conseil.

1.3. Diagnostiquer et piloter l'évolution des architectures et de l'urbanisation des SI (8h)

- **Schéma pédagogique proposé**

Phase 1 (2h) : Cours magistral — Urbanisation et cartographie des SI (couches métier, fonctionnelle, applicative, technique) ; outils de modélisation (BPMN, ArchiMate, MEGA) ; interopérabilité des SI (EAI, ETL, API REST, formats XML/JSON) ; technologies émergentes et leur impact sur les architectures (IA, blockchain, IoT, RPA) ; enjeux d'intégrité, traçabilité, auditabilité.

Phase 2 (3h) : TD cartographie — À partir d'un SI fictif d'une PME industrielle (ERP, CRM, WMS, portail client) : réaliser une cartographie applicative simplifiée en couches, identifier les flux d'information critiques, repérer les points de rupture et les risques d'interopérabilité. Utilisation d'un outil de modélisation libre (draw.io).

Phase 3 (3h) : Cas technologie — Analyse de l'opportunité d'intégrer une solution blockchain dans une chaîne d'approvisionnement : fonctionnement, usages (traçabilité, smart contracts), avantages, limites, impacts organisationnels et réglementaires. Recommandation argumentée pour la direction.

- **Cas pratique type DSCG**

La coopérative AGRI-CONNECT — Modernisation de l'architecture SI et intégration de l'IA

Contexte : AGRI-CONNECT est une coopérative agricole (CA 85 M€, 12 sites de collecte, 1 200 adhérents) dont le SI est constitué d'un ERP vieillissant (Sage 100), de tableurs Excel pour la gestion des stocks, d'une application mobile adhérents développée en 2019 et d'un portail web de commande non connecté à l'ERP. La direction envisage une modernisation par étapes, incluant l'intégration de capteurs IoT dans les silos de stockage, le déploiement d'un module IA prédictive pour anticiper les récoltes et la mise en place d'une blockchain pour certifier l'origine des produits à destination des distributeurs.

Travail demandé :

1. Réaliser une cartographie applicative de l'architecture SI actuelle d'AGRI-CONNECT (annexe 1) : identifier les 4 couches (métier, fonctionnelle, applicative, technique), les flux d'échange entre systèmes et les zones d'hétérogénéité ou d'absence d'intégration.

2. Analyser les enjeux d'interopérabilité liés à la modernisation envisagée : quels protocoles et formats d'échange recommander pour connecter l'ERP, l'application mobile, les capteurs IoT et le futur module IA ? Identifier les risques d'intégrité et de cohérence des données.

3. Évaluer la pertinence d'un projet blockchain pour AGRI-CONNECT : fonctionnement du registre distribué dans ce contexte, type de blockchain recommandé (publique, privée, hybride), cas d'usage précis (certification d'origine, traçabilité, smart contracts fournisseurs), limites et risques.

4. Analyser les impacts organisationnels et comptables de l'intégration de l'IA prédictive pour la gestion des récoltes : transformation des processus décisionnels, évolution des compétences, enjeux de fiabilité et d'auditabilité des recommandations algorithmiques, cadre réglementaire (IA Act).

5. Proposer un plan de modernisation en 3 étapes, en précisant pour chaque étape : les technologies concernées, les dépendances, les risques, les critères de succès et les impacts sur les processus comptables et financiers de la coopérative.

Annexes : Annexe 1 : Schéma SI simplifié actuel (ERP, tableurs, app mobile, portail web) — Annexe 2 : Données IoT collectées par les capteurs pilotes (température, humidité, tonnage) — Annexe 3 : Extrait du cahier des charges du projet blockchain fournisseurs — Annexe 4 : Résultats du module IA prédictif sur la campagne N (récoltes estimées vs réelles) — Annexe 5 : Grille d'évaluation des technologies émergentes (à compléter).

1.4. Gérer les relations contractuelles et opérationnelles avec les ESN (6h)

- **Schéma pédagogique proposé**

Phase 1 (1h30) : Cours magistral — Typologies de prestations ESN (infogérance, TMA, intégration, cloud, cybersécurité) ; SLA et indicateurs de performance contractuelle ; clauses critiques (réversibilité, propriété intellectuelle, RGPD, sécurité) ; risques contractuels (dépendance, non-conformité, vendor lock-in) ; Code des marchés publics pour entités publiques.

Phase 2 (2h30) : TD analyse contractuelle — Analyse d'un contrat d'infogérance fictif (8 pages) : identifier les clauses protectrices et les zones de risque, vérifier la cohérence des SLA avec les besoins métier, repérer les lacunes en matière de RGPD et de réversibilité. Grille d'analyse structurée en binômes.

Phase 3 (2h) : Simulation de négociation — Jeu de rôle : une équipe représente un client (DSI d'une ETI), l'autre une ESN. Négociation sur 3 clauses critiques (SLA, réversibilité, propriété des données). Restitution collective et discussion sur les bonnes pratiques contractuelles.

- **Cas pratique type DSCG**

La société INDUS-PROCESS — Audit contractuel d'un contrat d'infogérance SI

Contexte : INDUS-PROCESS est un équipementier industriel (CA 65 M€, 350 salariés) ayant externalisé l'intégralité de son SI à une ESN (SOFTTEC) il y a 5 ans via un contrat d'infogérance globale (ERP, infrastructure, helpdesk, cybersécurité). Le DAF, récemment nommé, constate une dégradation de la qualité de service (incidents récurrents non traçés, temps de réponse dépassés, facturation opaque), et découvre que le contrat arrive à échéance dans 8 mois. Il mandate un cabinet d'expertise comptable pour réaliser un audit contractuel et préparer une nouvelle négociation ou un changement de prestataire.

Travail demandé :

1. Analyser le contrat d'infogérance en cours (annexe 1) sur 5 dimensions : périmètre des prestations, SLA et pénalités, clauses RGPD et sécurité, réversibilité et portabilité, propriété intellectuelle et des données. Identifier les lacunes et risques pour INDUS-PROCESS.

2. Évaluer la conformité du contrat au regard du RGPD : existe-t-il une clause de sous-traitance de données personnelles ? Les obligations du sous-traitant

(article 28 RGPD) sont-elles correctement formalisées ? Identifier les 3 principaux manquements.

3. Calculer le coût réel de l'infogérance sur 5 ans à partir des données de l'annexe 2 (coûts contractuels + pénalités non appliquées + coûts cachés estimés). Comparer avec le benchmark sectoriel et évaluer l'impact financier des défaillances de SOFTTEC.

4. Préparer le plan de sortie de contrat : identifier les conditions de réversibilité, les risques de migration (perte de données, continuité d'activité), les actions à engager dans les 8 prochains mois, les garanties à exiger du prestataire sortant.

5. Rédiger les 5 clauses prioritaires à intégrer dans le futur contrat d'infogérance, en justifiant pour chacune son importance au regard des dysfonctionnements constatés et des risques identifiés.

Annexes : Annexe 1 : Extrait du contrat d'infogérance SOFTTEC (15 clauses) — Annexe 2 : Tableau des incidents et SLA sur 24 mois — Annexe 3 : Facturation SOFTTEC N-1 et N (postes de coûts détaillés) — Annexe 4 : Benchmark sectoriel infogérance (coûts et SLA typiques ETI industrielles) — Annexe 5 : Grille d'audit contractuel (14 critères, à compléter).

1.5. Planifier, organiser et conduire des projets de systèmes d'information (6h)

- **Schéma pédagogique proposé**

Phase 1 (2h) : Cours magistral — Principes fondamentaux de la gestion de projet SI (cadrage, planification, suivi, clôture) ; méthodes comparées (cycle en V vs agile/Scrum vs hybride) ; acteurs et rôles (MOA, MOE, RACI) ; plan qualité et plan de tests ; gestion des risques (AMDEC, cartographie) ; indicateurs de performance projet (délais, coûts, valeur créée, satisfaction) ; facteurs clés d'échec (rapport Chaos).

Phase 2 (2h) : TD planification — À partir d'un cahier des charges partiel d'un projet de migration ERP (250 jours, 8 lots, 12 acteurs) : construire un GANTT simplifié, établir un RACI, identifier les tâches critiques (chemin critique), proposer 3 indicateurs de suivi. Travail en binômes avec outil tableur.

Phase 3 (2h) : Cas diagnostic — Analyse post-mortem d'un projet SI en difficulté (annexe) : identifier les causes de dépassement (délais, budget, périmètre), évaluer la qualité du pilotage, proposer des mesures correctives et rédiger une note de diagnostic structurée pour le comité de pilotage.

- **Cas pratique type DSCG**

La société MEDICA-PLUS — Pilotage d'un projet de migration vers un nouveau logiciel métier

Contexte : MEDICA-PLUS est un réseau de 18 pharmacies indépendantes regroupées en centrale d'achats (CA groupé 42 M€, 120 collaborateurs). Le groupement a décidé de migrer vers un nouveau logiciel de gestion pharmaceutique (LGO) intégrant la dispensation médicamenteuse, la gestion des stocks, la facturation Sécurité Sociale et un module de fidélisation client. Le projet, lancé il y a 6 mois, est déjà en retard de 3 mois sur le planning initial : le prestataire SI (ESN PHARMASYS) invoque des modifications tardives du cahier des charges, tandis que la MOA signale des fonctionnalités manquantes et un taux de bugs critiques élevé. Le cabinet d'expertise comptable du groupement est mandaté pour un audit de projet.

Travail demandé :

1. Analyser le plan de projet initial (annexe 1) et la situation actuelle : identifier les écarts (délais, budget, périmètre), quantifier les dépassements et qualifier les causes (défaillances MOA, MOE, communication, gestion des risques, qualité du cahier des charges).

2. Évaluer la qualité du plan qualité et du plan de tests du projet (annexe 2) : est-il conforme aux bonnes pratiques (couverture fonctionnelle, responsabilités, critères d'acceptation, procédures de recette) ? Identifier les 4 lacunes principales.

3. Réaliser une analyse des risques résiduels du projet à l'aide d'une cartographie AMDEC : identifier les 5 risques critiques (probabilité × impact), leur gravité et les plans de mitigation associés.

4. Proposer un plan de reprise en 3 phases : actions immédiates (30 jours) pour stabiliser le projet, actions de fond (60-90 jours) pour retrouver l'alignement avec les objectifs, et conditions de clôture réussie. Préciser les indicateurs de suivi.

5. Formuler des recommandations sur la gestion contractuelle avec PHARMASYS : quelles clauses auraient dû être incluses dans le contrat initial ? Quels recours sont envisageables face aux défaillances constatées (pénalités, résiliation, garanties) ?

Annexes : Annexe 1 : Plan de projet initial (GANTT, lots, jalons, budget) vs situation réelle au T+6 mois — Annexe 2 : Plan qualité et plan de tests PHARMASYS — Annexe 3 : Journal des anomalies (50 bugs classifiés) — Annexe 4 : Extrait du contrat MOA/MOE — Annexe 5 : Procès-verbal des comités de pilotage (3 derniers mois).

1.6. Mettre en œuvre et piloter la gestion des connaissances au sein du SI (6h)

- **Schéma pédagogique proposé**

Phase 1 (2h) : Cours magistral — Définitions et typologies des connaissances (tacites vs explicites, modèle SECI de Nonaka & Takeuchi) ; processus du Knowledge Management (acquisition, structuration, stockage, diffusion, capitalisation) ; rôle des SI dans la gestion des connaissances (GED, intranets, SharePoint, Notion, IA générative) ; gouvernance des connaissances (rôles, politiques, RGPD) ; enjeux du turn-over et des silos informationnels.

Phase 2 (2h) : TD cartographie — Cartographier les connaissances critiques d'un cabinet comptable type (20 collaborateurs) : distinguer connaissances tacites et explicites, identifier les porteurs de savoirs critiques, les risques liés aux départs, et proposer un dispositif de capitalisation adapté (wiki interne, base documentaire, mentorat, etc.).

Phase 3 (2h) : Cas diagnostic — Évaluation d'un dispositif KM existant (extraits d'une politique de gestion documentaire) : identifier les lacunes (silos, absence de mise à jour, inaccessibilité, risques RGPD), proposer un plan d'amélioration intégrant les outils collaboratifs actuels et les possibilités offertes par l'IA générative pour la recherche et la synthèse documentaire.

- **Cas pratique type DSCG**

Le cabinet AUDIT-EXPERTISE — Mise en place d'un dispositif de Knowledge Management

Contexte : AUDIT-EXPERTISE est un cabinet d'expertise comptable et de commissariat aux comptes (55 collaborateurs, 4 associés, 380 dossiers clients). Suite à 4 départs de managers en 18 mois — dont le départ du directeur technique, seul détenteur des méthodologies d'audit spécifiques du cabinet — et à une croissance rapide (intégration de 2 cabinets secondaires), la Direction s'inquiète de la perte de savoir-faire et des risques de discontinuité dans les missions. Par ailleurs, les nouveaux collaborateurs se plaignent d'une documentation interne lacunaire, de procédures non standardisées et d'outils collaboratifs peu utilisés (SharePoint configuré mais vide, wiki interne abandonné). La Direction souhaite formaliser une stratégie de Knowledge Management.

Travail demandé :

1. Réaliser un diagnostic de la gestion des connaissances au sein du cabinet à partir des éléments fournis en annexe : identifier les connaissances

critiques (tacites et explicites), les porteurs de savoirs clés, les silos informationnels et les points de vulnérabilité liés aux départs.

2. Proposer une cartographie des connaissances du cabinet structurée en 4 domaines : expertise technique (audit, fiscalité, comptabilité), méthodologies et processus internes, relations clients, connaissances réglementaires. Pour chaque domaine, identifier le niveau de formalisation actuel et les risques associés.

3. Concevoir un dispositif de Knowledge Management adapté à la taille et aux besoins du cabinet : choix des outils (GED, wiki, base de connaissances, IA de recherche), rôles à désigner (champion KM, responsables par domaine), politique de mise à jour, gouvernance RGPD des documents clients.

4. Évaluer les opportunités et les risques liés à l'utilisation de l'IA générative dans la gestion des connaissances du cabinet : gains d'efficacité (synthèse, recherche documentaire, onboarding), risques (hallucinations, confidentialité des données clients, dépendance à l'outil, responsabilité professionnelle).

5. Rédiger un plan d'action en 3 phases (0-3 mois : urgences, 3-9 mois : structuration, 9-18 mois : déploiement complet) pour mettre en place le dispositif KM. Préciser les ressources mobilisées, les livrables attendus et les indicateurs de suivi.

Annexes : Annexe 1 : Résultats de l'enquête interne sur la gestion des connaissances (45 réponses) — Annexe 2 : Inventaire des documents et outils SI existants (SharePoint, wiki, messagerie, Drive) — Annexe 3 : Liste des compétences critiques identifiées par les associés — Annexe 4 : Extrait de la politique de confidentialité clients (RGPD) — Annexe 5 : Grille d'évaluation du dispositif KM (12 critères, à compléter).

2. Organiser, exploiter et sécuriser les données de l'organisation (36h)

2.1. Concevoir l'organisation des données et assurer leur interopérabilité (14h)

- **Schéma pédagogique proposé**

Phase 1 (4h) : Cours magistral — Modèles de données (MCD, MLD, schémas relationnels ; le modèle relationnel est un prérequis important) ; cycles de transaction et données métier (FEC, EDI) ; architectures BI (entrepôt vs lac de données) ; standards d'interopérabilité (XBRL, JSON, EDI).

Phase 2 (5h30) : TD — Conception d'un MCD à partir d'un cas comptable simple (entreprise avec clients, fournisseurs, produits). Validation de l'interopérabilité avec un FEC.

Phase 3 (4h30) : Cas pratique — Audit d'un projet d'interconnexion de SI (ERP + outil métier) : identifier les flux de données, les standards utilisés, les risques de désalignement. Recommandations en termes de gouvernance des interfaces.

- **Cas pratique type DSCG**

Le groupe DISTRIB+ — Refonte de l'architecture de données pour interopérabilité avec les filiales

Contexte : DISTRIB+ est un groupe de distribution spécialisée (12 filiales en France et en Europe, CA consolidé de 380 M€) qui s'appuie sur 4 ERP différents hérités d'opérations de croissance externe successives. Le DAF souhaite consolider mensuellement les données financières en J+5 (vs J+15 aujourd'hui), tout en respectant les obligations FEC nationales spécifiques à chaque pays. Le DSI propose une couche de data warehouse unifiée. Les enjeux : interopérabilité technique, standardisation des plans comptables, conformité multi-juridictions.

Travail demandé :

1. Modéliser le schéma de données cible (MCD simplifié) du data warehouse permettant la consolidation financière de DISTRIB+. Identifier les entités, attributs et cardinalités principales.

2. Décrire le format FEC français et identifier les écarts probables avec les standards comptables italien et espagnol des filiales. Proposer une procédure de mapping.

3. Comparer une architecture data lake (stockage brut multi-sources) et data warehouse (modélisation cible) pour le besoin de DISTRIB+. Recommander un choix justifié.

4. Identifier les risques de réversibilité contractuelle si le data warehouse est hébergé en SaaS (ex. Snowflake). Proposer 4 clauses contractuelles à insérer (en s'appuyant sur les recommandations CIGREF).

5. Élaborer une feuille de route en 3 jalons (3 mois, 9 mois, 18 mois) pour la mise en œuvre du projet, avec acteurs, livrables et indicateurs de succès.

Annexes : Annexe 1 : Plans comptables actuels des 12 filiales (extrait) — Annexe 2 : Volumétrie estimée (millions de lignes/mois) — Annexe 3 :

Cartographie SI cible (à compléter) — Annexe 4 : Modèle de clauses cloud du CIGREF — Annexe 5 : Référentiel FEC officiel (DGFiP).

2.2. Collecter, traiter, analyser et interpréter des données à des fins décisionnelles (14h)

- **Schéma pédagogique proposé**

Phase 1 (2h30) : Cours magistral — Chaîne de valeur des données (de la collecte à la décision) ; data analytics descriptif / prédictif / prescriptif ; ETL et qualité des données ; data mining (classification, clustering, scoring) ; pilotage par la donnée (KPI, BSC, OKR, rolling forecast) ; data storytelling.

Phase 2 (3h30) : TP Excel et Power BI — Tableaux croisés dynamiques avancés sur balance analytique (500 lignes) ; Power Pivot et mesures DAX ; conception d'un rapport Power BI complet (connexion, Power Query, modèle relationnel, 5 visualisations, publication).

Phase 3 (2h30) : TD analytique — Construction d'un Balanced Scorecard pour entreprise industrielle (4 axes, KPI SMART) ; passage budget annuel → rolling forecast ; sélection d'indicateurs ESG conformes CSRD ; analyse multidimensionnelle d'un jeu de données réel.

Phase 4 (2h30) : TD diagnostic et décision — Critique de visualisations (8 cas, bonnes/mauvaises pratiques) ; calcul VAN/TRI sur 3 projets concurrents ; arbre de décision avec scénarios probabilisés ; identification de biais cognitifs.

Phase 5 (3h) : Cas pratique intégré — Mise en situation type DSCG : du fichier brut au tableau de bord exécutif et à la recommandation argumentée.

- **Cas pratique type DSCG**

La société TECH-SOLUTIONS — De l'analyse de rentabilité au choix d'investissement

Contexte : TECH-SOLUTIONS est une ESN (120 salariés, CA 14 M€) spécialisée dans les projets de transformation digitale pour les PME. La direction constate des écarts importants de rentabilité entre projets et envisage simultanément deux investissements : (A) déploiement d'une suite Power BI et data warehouse (250 k€) et (B) recrutement de 4 consultants seniors avec hausse de l'effort commercial (380 k€). Le contrôleur de gestion dispose d'un fichier Excel de 800 lignes d'imputations de temps et d'une base de facturation. Le DAF doit présenter une recommandation au Comité Stratégique sur (1) la situation actuelle, (2) le choix d'investissement, (3) le pilotage futur.

Travail demandé :

1. À partir du fichier Excel fourni (annexe 1), construire un tableau croisé dynamique analysant la rentabilité par projet et par consultant. Identifier les anomalies (valeurs manquantes, doublons, heures aberrantes) et proposer une procédure de nettoyage.

2. Concevoir la structure d'un dashboard Power BI synthétisant les indicateurs clés : 3 pages thématiques (rentabilité, charge consultants, prévisionnel), visualisations recommandées, filtres temporels. Justifier les choix de représentation au regard des bonnes pratiques de data storytelling.

3. Calculer la VAN et le TRI des projets A et B sur 5 ans (taux d'actualisation 9 %, données en annexe 2). Construire un arbre de décision intégrant deux scénarios (optimiste 40 %, pessimiste 60 %) pour chaque projet. Identifier 3 biais cognitifs susceptibles d'altérer le choix.

4. Concevoir un Balanced Scorecard pour TECH-SOLUTIONS intégrant 8 KPI répartis sur les 4 axes (financier, client, processus, apprentissage), avec au moins 2 indicateurs ESG. Formuler des objectifs SMART pour les 3 KPI les plus stratégiques.

5. Rédiger une note de synthèse d'une page (format CODIR) présentant : (a) le diagnostic de la situation actuelle, (b) le projet recommandé avec justification, (c) le dispositif de pilotage proposé pour les 12 prochains mois (rolling forecast trimestriel, indicateurs, gouvernance).

Annexes : Annexe 1 : Extrait du fichier Excel d'imputations (100 lignes avec anomalies intentionnelles) — Annexe 2 : Flux de trésorerie prévisionnels des projets A et B (5 ans, 2 scénarios) — Annexe 3 : Données de facturation par projet (N-1 et N) — Annexe 4 : Politique de confidentialité RH (RGPD) — Annexe 5 : Grille Balanced Scorecard à compléter — Annexe 6 : Référentiel CSRD — indicateurs sectoriels services.

2.3. Élaborer et piloter la gouvernance stratégique des données (8h)

- **Schéma pédagogique proposé**

Phase 1 (1h) : Cours magistral — Cycle de vie des données (7 étapes : création → suppression) ; rôles (data owner, data steward, DPO, RSSI, CDO) ; gouvernance information / données / SI ; modèle des 3 lignes de maîtrise.

Phase 2 (1h) : Cours magistral — Big Data (5V), architectures cloud (IaaS/PaaS/SaaS), datacenters et impacts ; qualité des données (ISO 25012) ; sécurité (CIA), archivage électronique ; normes ISO 27001/27005, RGPD, NIS2, DORA.

Phase 3 (1h) : Cours magistral — Actifs numériques : typologie (logiciels, brevets, cryptoactifs, NFT, tokens) ; cadres comptables (IAS 38, IFRS 3, PCG, ANC 2020-05 et 2026-02) ; risques spécifiques. Cadre réglementaire UE : Data Act, DGA, DSA, DMA, MiCA.

Phase 4 (2h30) : TD audit — Audit d'un dispositif de gouvernance des données : grille en 4 dimensions (ownership, lineage, métadonnées, catalog). Évaluation de la qualité d'un jeu de données (ISO 25012). Plan de mise en conformité ISO 27001.

Phase 5 (2h30) : Cas pratique intégré — Cas comportant audit RGPD + comptabilisation d'actifs numériques + analyse de monétisation conforme. Mise en situation type DSCG complète.

- **Cas pratique type DSCG**

La société PHARMA-LAB — Gouvernance des données, certification ISO 27001 et valorisation des actifs numériques

Contexte : PHARMA-LAB est un laboratoire pharmaceutique (CA 90 M€, 400 salariés) sous-traitant pour 3 grands donneurs d'ordres. Ces derniers exigent désormais la certification ISO 27001. Un audit de maturité révèle plusieurs lacunes : aucun data owner désigné, qualité des données R&D insuffisante (25 % de champs vides), politique d'archivage absente. En parallèle, le laboratoire détient un portefeuille d'actifs numériques significatif (2 logiciels propriétaires de simulation R&D développés en interne pour 800 k€, 3 brevets logiciels, et envisage de rejoindre un consortium blockchain de traçabilité des médicaments avec émission de tokens utilitaires). Le commissaire aux comptes prépare la certification N+1.

Travail demandé :

1. Auditer le dispositif de gouvernance des données existant sur 4 dimensions : data ownership, data lineage, gestion des métadonnées, data catalog. Identifier les 5 lacunes prioritaires et hiérarchiser.

2. Évaluer la qualité des données R&D (annexe 2) selon 6 critères ISO 25012 : exactitude, complétude, unicité, cohérence, actualité, accessibilité. Calculer les indicateurs et identifier 3 actions correctives prioritaires.

3. Proposer un plan de mise en conformité ISO 27001 : périmètre du SMSI, politiques à créer (PSSI, gestion des accès, gestion des incidents), rôles à désigner, calendrier sur 12 mois. Recommander une politique d'archivage électronique conforme aux exigences pharmaceutiques (BPF/ICH Q10).

4. Identifier et classifier comptablement les actifs numériques de PHARMA-LAB : logiciels propriétaires (IAS 38, PCG), brevets logiciels (test de

dépréciation), futurs tokens utilitaires (ANC 2020-05 et 2026-02). Proposer le traitement comptable adapté pour chaque catégorie.

5. Le laboratoire envisage de monétiser ses données R&D anonymisées via une plateforme partenariale. Vérifier la conformité RGPD du projet (base légale, anonymisation effective, droits des personnes), évaluer l'impact du Data Act, et formuler 5 recommandations pour un projet conforme et éthique.

Annexes : Annexe 1 : Rapport d'audit de maturité gouvernance (12 critères, scores 1-5) — Annexe 2 : Audit qualité données R&D (extrait base de 100 enregistrements) — Annexe 3 : Portefeuille d'actifs numériques au 31/12/N (logiciels, brevets, projet tokens) — Annexe 4 : Extraits règlements ANC 2020-05 et 2026-02 — Annexe 5 : Description du projet de monétisation (catalogue de données R&D) — Annexe 6 : Grille ISO 27001 (à compléter) — Annexe 7 : Extraits BPF/ICH Q10 sur archivage pharmaceutique.

3. Mettre en œuvre les outils SI au service de la performance organisationnelle (20h)

3.1. Concevoir, construire et exploiter des outils de pilotage de la performance (8h)

- **Schéma pédagogique proposé**

Phase 1 (1h30) : Cours magistral — Principes du contrôle de gestion appliqués aux SI ; typologie des coûts (CAPEX/OPEX, directs/indirects, cachés) ; méthode TCO (Total Cost of Ownership) ; méthode ABC adaptée aux SI ; calcul du ROI d'un projet SI ; indicateurs de pilotage (techniques, économiques, gouvernance, ESG).

Phase 2 (2h) : TD analyse de coûts — À partir d'un dossier de coûts informatiques d'une ETI (factures, contrats prestataires, masse salariale SI, amortissements) : reconstituer le TCO sur 3 ans, identifier les coûts cachés (formation, perte de productivité, interruptions), comparer avec un benchmark sectoriel et formuler des recommandations d'optimisation.

Phase 3 (2h) : TD construction de tableau de bord — Conception d'un tableau de bord SI selon une démarche structurée (Balanced Scorecard adaptée) : sélection de 12 KPI répartis en 4 axes (technique, économique, gouvernance, ESG), définition des formules de calcul, sources de données, fréquences de mise à jour et seuils d'alerte. Travail en groupes, restitution croisée.

Phase 4 (2h30) : Cas synthèse — Évaluation critique d'un dispositif de contrôle de gestion SI existant (annexes fournies) : identifier les faiblesses (indicateurs non pertinents, absence de KPI ESG, données obsolètes),

proposer un plan d'amélioration et une nouvelle maquette de tableau de bord. Restitution orale en 5 minutes.

- **Cas pratique type DSCG**

Le groupe INDUSTECH — Mise en place d'un dispositif de contrôle de gestion SI

Contexte : INDUSTECH est un groupe industriel de mécanique de précision (CA 95 M€, 4 sites de production, 520 collaborateurs). La fonction SI emploie 12 personnes et représente un budget annuel de 3,8 M€ (3,9 % du CA), perçu par la Direction Générale comme « élevé et opaque ». Le DAF, qui a hérité du suivi budgétaire SI il y a 18 mois, constate que les écarts budgétaires SI atteignent +18 % sans qu'aucune analyse de cause ne soit produite, qu'aucun TCO n'a jamais été établi pour les principales applications (ERP, MES, GED) et que le seul reporting existant est un tableau Excel mensuel listant les factures par fournisseur. Le Comité de Direction mandate un cabinet d'expertise comptable pour structurer le contrôle de gestion SI et concevoir un tableau de bord adapté.

Travail demandé :

1. Cartographier la structure des coûts SI d'INDUSTECH à partir des annexes 1 et 2 : distinguer CAPEX et OPEX, coûts directs et indirects, coûts visibles et coûts cachés. Calculer le poids relatif de chaque poste et comparer au benchmark sectoriel fourni.

2. Calculer le TCO sur 3 ans des trois applications principales du groupe (ERP Sage X3, MES, GED) à partir des données de l'annexe 3. Identifier les postes de coûts les plus significatifs et les éventuels coûts cachés (formation, interruptions, dette technique).

3. Proposer une méthode de répartition analytique des coûts SI par centre de coûts et par activité (méthode ABC simplifiée) : identifier les inducteurs de coûts pertinents, modéliser la refacturation interne aux directions métiers, et illustrer la démarche sur deux processus (production et commercial).

4. Concevoir un tableau de bord SI structuré en 4 axes (Balanced Scorecard adapté) : performance technique (disponibilité, incidents), performance économique (TCO, ROI projets), gouvernance (alignement stratégique, satisfaction utilisateurs), durabilité (empreinte carbone, sobriété). Sélectionner 12 KPI mesurables avec formule, source, fréquence et seuil d'alerte.

5. Formuler 5 recommandations priorisées au Comité de Direction pour structurer le contrôle de gestion SI sur 18 mois : actions immédiates (3 mois),

structurelles (6-12 mois) et de fond (12-18 mois). Justifier la priorisation au regard des enjeux financiers, organisationnels et stratégiques du groupe.

Annexes : Annexe 1 : Budget SI N-2, N-1 et N par poste (matériel, logiciels, prestataires, masse salariale interne) — Annexe 2 : Liste des contrats SI en cours (15 contrats : ERP, infogérance, télécoms, cybersécurité, licences) — Annexe 3 : Données de coûts détaillées des 3 applications principales (acquisition, maintenance, formation, incidents) — Annexe 4 : Benchmark sectoriel mécanique de précision (ratios SI/CA, structure type des coûts) — Annexe 5 : Extrait du dernier reporting SI mensuel (à critiquer).

3.2. Auditer, contrôler et évaluer la performance et la conformité des SI (8h)

- **Schéma pédagogique proposé**

Phase 1 (2h) : Cours magistral — Définition et périmètre de l'audit SI ; distinction audit SI / audit financier ; normes NEP applicables (NEP 240, 260, 315, 330, 500) ; référentiels (COBIT, ISO 27001, ITIL) ; étapes d'une mission d'audit SI (cadrage, cartographie des risques, programme de travail, collecte de preuves, restitution) ; articulation avec la certification légale des comptes.

Phase 2 (2h) : TD cartographie des risques SI — À partir d'une description d'organisation et de SI : élaborer une cartographie des risques SI selon une grille probabilité × impact, identifier 8 à 10 risques majeurs (gestion des accès, sauvegardes, intégrité des données, dépendance fournisseur, etc.), prioriser et formuler un programme d'audit thématique de 5 jours.

Phase 3 (2h) : TD audit thématique — Conduite d'un audit thématique sur un processus SI sensible (gestion des accès aux applications comptables) : check-lists d'audit, entretiens simulés (jeu de rôles), analyse de logs fournis, identification des constats, formulation des recommandations selon une grille standardisée (constat, risque, recommandation, priorité, échéance).

Phase 4 (2h) : Cas rédactionnel — Rédaction d'une note de synthèse d'audit SI à destination d'un comité d'audit : structure type (objet, contexte, méthodologie, constats, recommandations), hiérarchisation des messages, vocabulaire adapté au décideur. Restitution écrite (4-5 pages maximum) suivie d'une critique croisée.

- **Cas pratique type DSCG**

Le groupe MEDIA-PARTNERS — Audit SI dans le cadre de la certification légale des comptes

Contexte : MEDIA-PARTNERS est un groupe média et communication coté sur Euronext Growth (CA 145 M€, 3 filiales, 720 collaborateurs). Son commissaire aux comptes (CAC) a identifié, lors de l'évaluation préliminaire du contrôle interne (NEP 315), plusieurs zones de risque SI significatives : le SI comptable repose sur un ERP fortement paramétré ayant subi 4 montées de version en 18 mois, les droits d'accès n'ont pas été revus depuis 30 mois, plusieurs interfaces automatiques entre applications métier et comptabilité fonctionnent sans piste d'audit fiable, et un incident de sauvegarde non détecté pendant 5 jours a été révélé en interne. Le CAC mandate son équipe d'audit SI pour une mission ciblée préalable à la certification des comptes N. L'expertise comptable du groupe est associée à la mission pour faciliter l'accès aux données.

Travail demandé :

1. Élaborer une cartographie des risques SI de MEDIA-PARTNERS à partir des annexes 1 et 2 : identifier 10 risques selon les axes intégrité, disponibilité, confidentialité et auditabilité, les évaluer (probabilité × impact) et les hiérarchiser. Justifier la cotation au regard des enjeux de certification des comptes.

2. Définir le programme d'audit SI à conduire sur 8 jours-hommes pour répondre aux exigences NEP 315 : périmètre, processus à auditer en priorité, livrables attendus, articulation avec les travaux du commissaire aux comptes financier. Identifier les normes professionnelles mobilisables.

3. Évaluer la qualité de la piste d'audit fiable des interfaces automatiques entre applications métier et comptabilité (annexe 3). Identifier les faiblesses (absence de logs, données non horodatées, contrôles manquants) et leurs conséquences sur la fiabilité de l'information financière. Quel impact sur l'opinion du CAC ?

4. Analyser la gouvernance des accès aux applications sensibles (annexe 4) : conformité au principe de moindre privilège, séparation des tâches (notamment entre saisie et validation des écritures comptables), revues d'habilitations, gestion des départs. Identifier 5 manquements et leurs conséquences potentielles.

5. Rédiger une note de synthèse d'audit (4 pages maximum) à destination du Comité d'audit du groupe : présentation des constats prioritaires, évaluation globale du dispositif de contrôle interne SI, recommandations hiérarchisées avec délais, et conclusions sur l'incidence des constats sur la stratégie d'audit financier.

Annexes : Annexe 1 : Cartographie applicative simplifiée du groupe (8 applications principales et leurs interfaces) — Annexe 2 : Synthèse des incidents SI majeurs sur 24 mois (12 incidents documentés) — Annexe 3 :

Description des 4 interfaces automatiques métier-comptabilité (logs, contrôles, anomalies) — Annexe 4 : Extrait de la matrice des droits d'accès (50 utilisateurs sur l'ERP comptable) — Annexe 5 : Procès-verbal de l'incident de sauvegarde (chronologie, périmètre, mesures correctives) — Annexe 6 : Grille d'évaluation NEP 315 (à compléter).

3.3. Appréhender les usages et les enjeux des technologies de la blockchain et des cryptoactifs (4h)

- **Schéma pédagogique proposé**

Phase 1 (1h) : Cours magistral — Fondements techniques et fonctionnels de la blockchain (registre distribué, cryptographie, consensus, smart contracts) ; typologies (publique, privée, permissionnée, hybride) ; cas d'usage en expertise comptable et audit (piste d'audit fiable, certification d'actifs, traçabilité, automatisation) ; cadres réglementaires (MiCA, loi PACTE, eIDAS 2.0) ; cryptoactifs et leur traitement comptable (ANC 2020-05 et 2026-02).

Phase 2 (1h) : TD analyse d'opportunité — À partir de 3 cas sectoriels (supply chain agroalimentaire, gestion des dossiers patients, certification d'actifs immatériels) : évaluer la pertinence d'une solution blockchain selon une grille structurée (besoin réel vs effet de mode, choix de la typologie, alternatives, ROI estimé, risques). Restitution comparée.

Phase 3 (1h) : TD comptabilisation — Exercices de comptabilisation de cryptoactifs selon les règlements ANC 2020-05 et 2026-02 : achat de Bitcoin et Ether en trésorerie, plus-value de cession (méthode CMUP), token issu d'une ICO, NFT à l'actif. Articulation avec la fiscalité DGFiP des cryptoactifs.

Phase 4 (1h) : Cas synthèse — Évaluation d'un projet blockchain dans une mission d'audit : analyser un livre blanc de projet blockchain interne (traçabilité fournisseurs), identifier les forces et faiblesses, formuler un avis sur l'opportunité, et préciser les diligences d'audit applicables (NEP 315, NEP 500). Restitution orale en 5 minutes.

- **Cas pratique type DSCG**

La société TRACE-FOOD — Évaluation d'un projet blockchain de traçabilité alimentaire

Contexte : TRACE-FOOD est une coopérative agroalimentaire spécialisée dans les produits laitiers premium (CA 75 M€, 280 producteurs adhérents, 8 sites de transformation). Suite à plusieurs scandales sectoriels et à des exigences croissantes de la grande distribution, le directoire envisage le déploiement d'une solution blockchain de traçabilité « de la ferme au consommateur final » : enregistrement immuable des étapes de production,

smart contracts pour automatiser le paiement des producteurs au respect de cahiers des charges qualité, et accès consommateur via QR code. Le projet, estimé à 1,2 M€ d'investissement initial et 250 k€ annuels en exploitation, soulève des interrogations : une telle solution est-elle vraiment nécessaire ? Quelle blockchain choisir ? Quels impacts comptables et organisationnels ? Le commissaire aux comptes et l'expert-comptable du groupe sont mandatés pour produire un avis indépendant.

Travail demandé :

1. Évaluer la pertinence d'une solution blockchain pour le besoin de traçabilité de TRACE-FOOD : examiner si les caractéristiques distinctives de la blockchain (immutabilité, désintermédiation, consensus distribué) répondent à un besoin réel, ou si une base de données centralisée auditée suffirait. Justifier la conclusion.

2. Analyser le choix entre blockchain publique, privée et permissionnée pour ce projet : exposer les avantages et inconvénients de chaque typologie au regard des contraintes spécifiques (confidentialité des données producteurs, performance, coût, gouvernance multiparties prenantes). Recommander une typologie justifiée.

3. Identifier les risques juridiques et opérationnels du projet : protection des données personnelles (RGPD pour les producteurs et consommateurs), risque réglementaire MiCA si tokenisation envisagée, dépendance technologique, scalabilité, consommation énergétique, complexité de maintenance, articulation avec le droit français de la preuve.

4. Évaluer les impacts organisationnels et comptables du projet : transformation des processus métier (production, qualité, paiement des producteurs), évolution du contrôle interne, nouvelles compétences requises, traitement comptable de l'investissement (immobilisations incorporelles, charges d'exploitation), articulation avec les obligations de durabilité (CSRD).

5. Formuler un avis d'expert-comptable structuré au directoire : recommandation argumentée (engagement, ajournement, refus), conditions de succès et points de vigilance, articulation avec une éventuelle mission de commissariat aux comptes (incidence sur NEP 315 et NEP 500 en cas de mise en œuvre), et identification des indicateurs de pilotage à mettre en place pour suivre la valeur créée.

Annexes : Annexe 1 : Livre blanc du projet blockchain TRACE-FOOD (architecture cible, flux, parties prenantes) — Annexe 2 : Étude économique du projet (TCO 5 ans, ROI estimé, scénarios) — Annexe 3 : Analyse comparative de 3 solutions techniques (Hyperledger Fabric, blockchain publique Ethereum, base de données distribuée auditée) — Annexe 4 :

Cartographie des données traitées (données producteurs, qualité produit, traçabilité) — Annexe 5 : Extraits MiCA et règlement ANC 2020-05 — Annexe 6 : Grille d'évaluation d'opportunité blockchain (10 critères, à compléter).

4. Sécuriser et rendre durable le système d'information (36h)

4.1. Identifier, analyser et gérer les risques liés aux systèmes d'information (12h)

- **Schéma pédagogique proposé**

Phase 1 (3h) : Cours magistral — Typologie des risques liés aux SI (cyber, réglementaires, métier, projet) ; méthodes d'analyse (EBIOS Risk Manager, MEHARI, ISO 27005) ; cartographie des risques SI ; intégration dans la cartographie d'entreprise et le contrôle interne ; surveillance et indicateurs (KRI) ; reporting au conseil d'administration ; cadre réglementaire (RGPD, NIS2, DORA, NEP 240/260/315).

Phase 2 (3h) : TD application EBIOS — Application simplifiée de la méthode EBIOS Risk Manager sur un cas d'ETI : ateliers 1 (cadrage), 2 (sources de risques), 3 (scénarios stratégiques) et 4 (scénarios opérationnels). Restitution d'une cartographie de risques avec 6 scénarios documentés. Travail en groupes.

Phase 3 (3h) : TD impact financier et comptable — À partir d'un dossier d'incident cyber (ransomware ayant paralysé un ERP pendant 7 jours) : quantifier les conséquences sur la production des états financiers, identifier les écritures comptables impactées, évaluer les provisions pour dépréciation et engagements hors bilan, et apprécier l'incidence sur la continuité d'exploitation et le rapport de gestion.

Phase 4 (3h) : Cas conformité réglementaire — Évaluation de la conformité d'un dispositif de gestion des risques SI à un référentiel composite (NEP 315 + RGPD + NIS2) : analyse documentaire, identification des manquements, plan de remédiation priorisé, articulation entre obligations métier et obligations d'audit. Restitution écrite (note de synthèse de 3 pages).

- **Cas pratique type DSCG**

Le groupe ASSUR-PROTECTION — Cartographie des risques SI et impacts sur les états financiers

Contexte : ASSUR-PROTECTION est un courtier en assurances multirisques pour professionnels (CA 38 M€, 180 collaborateurs, portefeuille de 12 000 entreprises clientes). En tant qu'opérateur traitant des données financières et de santé sensibles, le groupe est soumis au RGPD strict, à la directive

NIS2 (entité essentielle depuis octobre 2024), aux exigences de l'ACPR pour son activité de courtage et à la certification légale de ses comptes. Trois événements récents inquiètent la direction : (1) une tentative de phishing ciblée sur la directrice financière, déjouée de justesse ; (2) la découverte que l'ERP métier conserve les données clients depuis l'origine du cabinet sans politique de purge ; (3) une note récente du CAC évoquant des « zones de risque significatif » sur le SI dans le cadre de NEP 315. Le directoire mandate un cabinet d'expertise comptable pour produire une cartographie consolidée des risques SI et évaluer leur impact sur les comptes.

Travail demandé :

1. Élaborer la cartographie des risques SI d'ASSUR-PROTECTION en mobilisant la méthode EBIOS Risk Manager : identifier 8 scénarios de risque selon les 4 typologies (cyber, réglementaire, métier, financier), évaluer chaque scénario (probabilité × impact), positionner les scénarios sur une matrice et hiérarchiser. Justifier la cotation au regard du contexte sectoriel.

2. Analyser l'impact potentiel des 3 risques majeurs identifiés sur la production et la fiabilité des états financiers : quels postes comptables seraient affectés ? Quels engagements hors bilan ? Quelle incidence sur la continuité d'exploitation ? Quelles provisions à constituer ? Argumenter à partir des règles du PCG et des NEP applicables.

3. Évaluer la conformité du dispositif actuel aux exigences réglementaires composites : RGPD (durée de conservation, registre, sécurité), NIS2 (signalement d'incidents sous 24h, mesures de gestion des risques), NEP 315 (couverture des risques SI dans le contrôle interne). Identifier 5 manquements prioritaires et leurs conséquences.

4. Apprécier les enjeux éthiques et déontologiques liés à l'éventuelle utilisation de l'IA générative pour le traitement des dossiers clients : risques de biais, de confidentialité, de responsabilité professionnelle, articulation avec le secret professionnel et le code de déontologie du courtier. Formuler des préconisations.

5. Construire un plan de remédiation des risques SI sur 18 mois articulé avec le calendrier d'audit légal : actions immédiates (0-3 mois) à porter à la connaissance du CAC, actions structurantes (3-12 mois) intégrant un dispositif de surveillance continue (KRI), et actions de fond (12-18 mois). Identifier les indicateurs de pilotage à reporter au conseil de surveillance et au CAC.

Annexes : Annexe 1 : Architecture SI simplifiée d'ASSUR-PROTECTION et inventaire des données traitées — Annexe 2 : Note du CAC sur les zones de risque SI identifiées dans le cadre de NEP 315 — Annexe 3 : Détail de l'incident de phishing (chronologie, mode opératoire, mesures prises) —

Annexe 4 : Extrait du registre des traitements RGPD (à analyser) — Annexe 5 : Synthèse des obligations NIS2 applicables aux entités essentielles — Annexe 6 : Grille d'analyse EBIOS Risk Manager (à compléter).

4.2. Concevoir, mettre en œuvre et contrôler une politique de sécurité des SI (12h)

- **Schéma pédagogique proposé**

Phase 1 (2h) : Cours magistral — Principes fondamentaux de la cybersécurité (CIA + traçabilité) ; politique de sécurité des SI (PSSI) ; charte informatique ; classification des actifs et des informations ; rôle du RSSI ; cadre réglementaire (NIS2, DORA, eIDAS 2, RGPD, LPM) ; norme ISO 27001 et ses 93 mesures de sécurité (Annexe A).

Phase 2 (2h30) : TD analyse de PSSI — À partir d'extraits de PSSI réelles (3 organisations : PME, ETI, grand groupe) : analyser la qualité, l'exhaustivité et l'application réelle, identifier les forces et faiblesses, comparer les approches selon la taille et le secteur, et proposer une trame de PSSI standard adaptée à une ETI.

Phase 3 (2h30) : TD architecture de confiance et IAM — Conception d'un dispositif de gestion des identités et des accès (IAM) pour une organisation type : matrice des rôles et habilitations, principe du moindre privilège, séparation des tâches sensibles (notamment en environnement comptable), authentification multifacteur, traçabilité, revues d'habilitations. Intégration de la signature électronique conforme eIDAS 2.

Phase 4 (3h) : TD PCA/PRA — Élaboration d'un plan de continuité d'activité simplifié pour un cabinet d'expertise comptable : analyse d'impact métier (BIA), identification des processus critiques, RTO/RPO, scénarios de sinistre, dispositif de sauvegarde et de reprise, modalités de test. Restitution du plan synthétisé en une note de 4 pages.

Phase 5 (2h) : Cas synthèse — Audit d'une politique de sécurité existante face aux exigences NIS2 / DORA : analyse de l'écart, identification des mesures à compléter, plan d'action de mise en conformité, articulation avec les obligations de signalement d'incidents et la gouvernance. Restitution orale en 5 minutes.

- **Cas pratique type DSCG**

Le cabinet FINANCE-EXPERTISE — Mise en œuvre d'une politique de cybersécurité conforme NIS2

Contexte : FINANCE-EXPERTISE est un cabinet d'expertise comptable et de commissariat aux comptes (160 collaborateurs, 5 bureaux régionaux, 850

dossiers clients dont 90 entités d'intérêt public). Considéré comme « entité essentielle » au sens de la directive NIS2 transposée en droit français en 2024 (en raison de son activité auprès d'OIV/OSE et de son volume), le cabinet doit se mettre en conformité avant la fin de l'exercice. L'audit préalable révèle une situation préoccupante : aucune PSSI formalisée, charte informatique signée par 60 % des collaborateurs seulement, absence de RSSI désigné (rôle assumé de fait par le « DSI » qui est en réalité un consultant externe à temps partiel), authentification simple sur tous les outils métier, sauvegardes non testées depuis 30 mois, et aucun PCA documenté. Par ailleurs, un incident de ransomware a touché un cabinet concurrent il y a 3 mois, conduisant à 2 semaines d'interruption d'activité et à une perte de 600 k€. Le directoire mandate un cabinet de conseil pour produire un plan de mise en conformité.

Travail demandé :

1. Élaborer la trame d'une politique de sécurité des systèmes d'information (PSSI) adaptée à FINANCE-EXPERTISE : structure (objectifs, périmètre, principes, organisation, mesures, gouvernance), contenus prioritaires, articulation avec la charte informatique et le code de déontologie professionnelle. Identifier les rôles à formaliser (RSSI, DPO, correspondants sécurité par bureau).

2. Concevoir un dispositif IAM (Identity and Access Management) répondant aux exigences spécifiques du métier : principe du moindre privilège, séparation des tâches sensibles (notamment dans le cadre de l'audit légal — séparation entre dossiers de signature et dossiers d'audit), authentification multi facteur, gestion du cycle de vie des accès (arrivée, mobilité, départ), revues semestrielles. Justifier les choix au regard de NEP 315 et du code de déontologie.

3. Construire une architecture de confiance pour les échanges dématérialisés du cabinet : signature électronique conforme eIDAS 2 (qualifiée pour la signature des comptes annuels par le commissaire aux comptes), horodatage qualifié, archivage à valeur probante, coffre-fort numérique pour les pièces clients. Identifier les prestataires qualifiés ANSSI à privilégier.

4. Élaborer un plan de continuité d'activité (PCA) pour le cabinet : identifier les processus critiques (production des arrêtés comptables en période fiscale, audits en cours, échéances DGFiP), définir les RTO et RPO, dimensionner le dispositif de sauvegarde et de reprise (sites de repli, sauvegardes hors ligne anti-ransomware, simulations annuelles). Préciser les indicateurs de pilotage du PCA.

5. Établir un plan de mise en conformité NIS2 sur 12 mois : actions de gouvernance (désignation du RSSI, gouvernance, comité sécurité), actions

techniques (segmentation, EDR, sauvegardes immuables), actions humaines (sensibilisation, formation, gestion des accès), et dispositif de signalement d'incidents (24h pour pré-notification, 72h pour notification complète à l'ANSSI). Évaluer le budget et les risques de non-conformité (sanctions financières prévues par NIS2).

Annexes : Annexe 1 : Cartographie SI actuelle de FINANCE-EXPERTISE (applications métier, infrastructure, prestataires) — Annexe 2 : Audit préalable de cybersécurité (16 constats classés par criticité) — Annexe 3 : Synthèse des obligations NIS2 pour entités essentielles — Annexe 4 : Catalogue des prestataires qualifiés ANSSI (PRIS, PASSI, PDIS) — Annexe 5 : Trame PSSI ANSSI (à adapter) — Annexe 6 : Grille d'auto-évaluation NIS2 (40 points de contrôle, à compléter).

4.3. Intégrer les enjeux de durabilité et de sobriété numérique dans le management des SI (12h)

- **Schéma pédagogique proposé**

Phase 1 (3h) : Cours magistral — Empreinte environnementale du numérique en France (chiffres ADEME/ARCEP) ; cadre réglementaire (loi REEN, CSRD/ESRS, taxonomie verte UE) ; principes du Green IT (IT for Green / Green for IT) ; sobriété numérique ; écoconception des services numériques (RGESN) ; ISO 14001 appliquée au SI ; articulation gouvernance SI / stratégie RSE.

Phase 2 (3h) : TD mesure d'empreinte — À partir d'un site web ou d'une application fournie : utiliser les outils EcoIndex et GreenIT Analysis pour évaluer la performance environnementale, identifier les principaux postes d'impact, formuler 5 préconisations d'écoconception et estimer les gains potentiels (tonnes équivalent CO_2 évitées). Travail en groupes.

Phase 3 (3h30) : TD reporting CSRD — Construction d'un volet « numérique » du reporting de durabilité d'une organisation soumise à CSRD : sélection des indicateurs ESRS pertinents (E1 climat — émissions Scope 1/2/3 du numérique, E5 ressources et économie circulaire — durabilité matérielle, S1 effectifs — fracture numérique), méthodes de collecte, articulation avec le bilan carbone numérique. Restitution d'un tableau de bord de durabilité numérique.

Phase 4 (3h30) : Cas stratégie SI durable — Conception d'un volet durabilité dans un schéma directeur des SI : axes (Green IT, sobriété, écoconception, achats responsables), trajectoire (3 ans), gouvernance (comité durabilité SI), indicateurs ESG, et articulation avec la stratégie RSE globale. Présentation orale en 5 minutes au CODIR fictif.

- **Cas pratique type DSCG**

Le groupe DURABLE-INDUSTRIES — Intégration du numérique dans le reporting CSRD et trajectoire de sobriété

Contexte : DURABLE-INDUSTRIES est un groupe industriel coté (CA 320 M€, 1 200 collaborateurs, 6 sites en France et en Europe) spécialisé dans les solutions d'efficacité énergétique pour le bâtiment. Soumis à la directive CSRD pour son exercice clos au 31 décembre N+1, le groupe doit produire son premier rapport de durabilité conforme aux normes ESRS, audité par un commissaire aux comptes dédié à la durabilité. La directrice RSE constate que le périmètre numérique est mal couvert : aucune mesure d'empreinte carbone du SI n'est disponible, les achats informatiques ne suivent aucun critère environnemental, et la flotte de 1 400 équipements (postes, smartphones, serveurs) est renouvelée tous les 3 ans sans politique d'allongement de la durée de vie. Le commissaire aux comptes durabilité, qui prépare ses diligences, a interrogé la direction sur la matérialité du sujet « numérique » dans la cartographie de durabilité du groupe. Le directeur des SI et la directrice RSE mandatent conjointement un cabinet d'expertise pour structurer une démarche de numérique responsable et alimenter le reporting CSRD.

Travail demandé :

1. Conduire une analyse de double matérialité (matérialité d'impact et matérialité financière) du sujet « numérique » pour DURABLE-INDUSTRIES selon la méthodologie ESRS 1 : identifier les impacts du SI sur l'environnement et la société, et les risques financiers du numérique pour le groupe (cybersécurité, obsolescence, dépendance énergétique). Conclure sur la matérialité du sujet et son intégration dans le rapport de durabilité.

2. Évaluer l'empreinte environnementale du SI du groupe à partir des données de l'annexe 2 (inventaire des équipements, consommation des datacenters, usages logiciels) en mobilisant la méthodologie ADEME / référentiel RGESN : calculer une estimation des émissions de gaz à effet de serre (Scope 1/2/3), identifier les principaux postes d'impact, et hiérarchiser les leviers de réduction.

3. Définir une politique de Green IT et de sobriété numérique pour le groupe : axes prioritaires (allongement de la durée de vie des équipements, écoconception, optimisation des datacenters, achats responsables), objectifs chiffrés à 3 ans, gouvernance (comité numérique responsable, rôles, indicateurs), articulation avec le label Numérique Responsable et la norme ISO 14001.

4. Élaborer le volet « numérique responsable » du tableau de bord de durabilité : sélectionner 8 indicateurs pertinents au regard des normes ESRS applicables (E1 climat, E5 économie circulaire, S1 effectifs propres),

préciser les formules, sources, fréquences et seuils. Identifier les indicateurs auditables et ceux soumis à appréciation qualitative.

5. Anticiper les diligences que conduira le commissaire aux comptes durabilité sur ce volet (NEP applicables au DPEF/CSRD) : nature des contrôles (auditabilité des données, fiabilité des sources, cohérence avec le système comptable), points de vigilance, et recommandations pour préparer la mission. Quel niveau d'assurance attendu (limité puis raisonnable) ?

Annexes : Annexe 1 : Cartographie SI du groupe et architecture des datacenters — Annexe 2 : Inventaire des équipements numériques (1 400 actifs) avec dates d'acquisition et consommation estimée — Annexe 3 : Politique d'achats actuelle (sans critères environnementaux) — Annexe 4 : Extrait du rapport RSE N-1 (sans volet numérique) — Annexe 5 : Synthèse ESRS E1, E5 et S1 applicables — Annexe 6 : Grille d'analyse de double matérialité (à compléter) — Annexe 7 : Référentiel RGESN (extrait, 20 critères prioritaires).

MATRICE DES REFERENTIELS

Cette section recense l'ensemble des référentiels normatifs, méthodes et cadres explicitement mentionnés dans le programme DSCG UE5 — Management des Systèmes d'Information dans sa version étendue de septembre 2025. Il a vocation à servir de boussole pédagogique aux enseignants pour construire séquences, études de cas et évaluations en s'appuyant sur des sources d'autorité reconnues.

L'inventaire est organisé en deux parties complémentaires :

- La première restitue les référentiels par catégorie thématique, en précisant pour chacun le nom complet, la source ou l'éditeur, et les sous-sections du programme où il est mobilisé.
- La seconde propose une matrice croisée référentiels × sections, présentée en orientation paysage pour permettre une lecture transversale d'un seul coup d'œil.

Trois précisions importantes guident la lecture de ce document :

- D'abord, le programme cite des référentiels selon trois logiques distinctes qu'il convient de ne pas confondre :
    - référentiels normatifs au sens strict (ISO, NEP, RGPD),
    - modèles théoriques (Henderson & Venkatraman, Kotter),
    - et catégories d'outils ou d'architectures (SIEM, IAM, IaaS).

  Le présent livret traite ces trois familles ensemble car toutes nourrissent l'enseignement, mais la distinction reste utile lorsqu'il s'agit d'évaluer la maîtrise attendue des candidats.
- Ensuite, certains acronymes techniques très usités (ETL, API, ERP, JSON, etc.) ne figurent pas dans cette matrice : ils relèvent du vocabulaire courant des SI et ne constituent pas des référentiels. Ils sont en revanche définis dans le glossaire du Guide pédagogique principal.
- Enfin, 3 absences notables méritent d'être signalées dès l'introduction :
    - les ISA (International Standards on Auditing), équivalents internationaux des NEP françaises ;
    - le référentiel COSO sur le contrôle interne, partenaire historique des NEP ;
    - et les méthodes de gestion de projet PMBOK et PRINCE2, alors même que les méthodes agiles sont citées. Une note

critique en fin de document propose des pistes de complément pédagogique sur ces points.

Chapitre 1 INVENTAIRE DES REFERENTIELS PAR CATEGORIE THEMATIQUE

Pour chaque catégorie, les référentiels sont présentés dans l'ordre où ils apparaissent dans le document source. La colonne « Sections » indique les sous-sections du programme DSCG UE5 où la mobilisation est explicite.

1. Normes professionnelles d'audit et de déontologie

Référentiels d'exercice professionnel des commissaires aux comptes et des experts-comptables. En contexte français, les normes professionnelles tiennent lieu d'équivalent aux ISA internationales.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
NEP 240	Responsabilité de l'auditeur en matière de fraude	*H2A / CNCC*	**3.2 · 4.1**
NEP 260	Communication avec le gouvernement d'entreprise sur le contrôle interne	*H2A / CNCC*	**4.1**
NEP 315	Connaissance de l'entité et de son environnement, dont le SI	*H2A / CNCC*	**3.2 · 4.1**
NEP 500	Caractère probant des éléments collectés	*H2A / CNCC*	**3.2 · 4.1**
NEP 9510	Diligences directement liées à la mission de CAC (audit SI)	*H2A / CNCC*	**3.2**
Code de déontologie	Code professionnel des experts-comptables et CAC	*CNOEC* *CNCC*	**4.1**
Code IFAC	Code international d'éthique des professionnels comptables	*IFAC*	**4.1**

2. Normes ISO mobilisables

Normes internationales applicables à la qualité, la sécurité, la durabilité, la continuité, la gouvernance et la qualité des données.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
ISO 8000	Qualité des données	*ISO*	**2.3**
ISO 9001	Systèmes de management de la qualité	*ISO*	**1.5 · 3.3**
ISO 14001	Systèmes de management environnemental	*ISO*	**3.3 · 4.3**
ISO/IEC 20000	Gestion des services informatiques	*ISO/IEC*	**3.2**
ISO/IEC 22301	Continuité d'activité	*ISO/IEC*	**3.3**
ISO/IEC 25012	Modèle de qualité des données	*ISO/IEC*	**2.2**
ISO 26000	Responsabilité sociétale des organisations	*ISO*	**4.3**
ISO/IEC 27001	Système de management de la sécurité de l'information (SMSI)	*ISO/IEC*	**2.3 · 3.2 · 3.3 · 4.2**
ISO/IEC 27701	Extension SMSI dédiée à la protection des données personnelles	*ISO/IEC*	**3.3**
ISO 31000	Management du risque — lignes directrices	*ISO*	**4.1**
ISO/IEC 38500	Gouvernance des technologies de l'information par l'entreprise	*ISO/IEC*	**1.2 · 3.2**

3. Référentiels de gouvernance et de management des SI

Cadres internationaux et modèles théoriques structurant l'alignement stratégique, la gouvernance et la maturité numérique.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
COBIT	Référentiel ISACA de gouvernance et de management des SI d'entreprise	*ISACA*	1.2 · 3.2
ITIL	Cadre de gestion des services informatiques (4e génération)	*AXELOS / Peoplecert*	1.2 · 1.5 · 3.2
CMMI	Capability Maturity Model Integration — modèle de maturité processus	*CMMI Institute / ISACA*	1.2 · 1.5
IT4IT	Architecture de référence du value stream IT	*The Open Group*	4.3
SDIA	Schéma directeur intégrant la durabilité	*Doctrine professionnelle*	4.3
Modèle Van Grembergen	Cadre de gouvernance SI (alignement, structure, processus, relationnel)	*Van Grembergen, De Haes (2009)*	1.2
Henderson & Venkatraman	Modèle d'alignement stratégique SI/métier	*IBM Systems Journal (1993)*	1.1
SAM	Strategic Alignment Model — déclinaison opérationnelle de Henderson & Venkatraman	*Henderson & Venkatraman (1993)*	1.1
IT Balanced Scorecard	Tableau de bord prospectif appliqué au SI	*Van Grembergen, Saull (2001)*	1.1 · 3.1
Digital Maturity Model	Modèles de maturité numérique (Deloitte, MIT)	*Deloitte / MIT Sloan*	1.2

Référentiel CIGREF	Publications CIGREF (MAGNum, modèle de valeur, gouvernance)	*CIGREF*	**1.1 · 1.2**

4. Cadres réglementaires européens et nationaux

Textes contraignants encadrant le traitement des données, la cybersécurité, l'IA, les cryptoactifs, la durabilité et la commande publique.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
RGPD	Règlement (UE) 2016/679 — protection des données personnelles	*Parlement européen et Conseil*	**1.3 · 2.2 · 2.3 · 3.2 · 4.1 · 4.2**
NIS 2	Directive (UE) 2022/2555 — cybersécurité dans l'Union	*Parlement européen et Conseil*	**1.3 · 3.2 · 4.1 · 4.2**
DORA	Règlement (UE) 2022/2554 — résilience opérationnelle numérique du secteur financier	*Parlement européen et Conseil*	**3.2**
MiCA	Règlement (UE) 2023/1114 — marchés de cryptoactifs	*Parlement européen et Conseil*	**1.3 · 3.2 · 3.3**
AI Act / IA Act	Règlement (UE) 2024/1689 — encadrement de l'intelligence artificielle	*Parlement européen et Conseil*	**1.3 · 4.1**
DGA	Data Governance Act — règlement (UE) 2022/868	*Parlement européen et Conseil*	**2.3**
DSA	Digital Services Act — règlement (UE) 2022/2065	*Parlement européen et Conseil*	**2.3**
ePrivacy	Directive 2002/58/CE — vie privée et	*Parlement européen et Conseil*	**2.3**

	communications électroniques		
eIDAS / eIDAS 2.0	Règlement (UE) 910/2014 et révision 2024 — identité numérique européenne	*Parlement européen et Conseil*	**3.3 · 4.1 · 4.2**
LPM	Loi de programmation militaire — protection des SI critiques	*République française*	**2.3 · 4.1 · 4.2**
Loi PACTE	Loi 2019-486 — encadrement des PSAN et cryptoactifs	*République française*	**3.3**
Code des marchés publics	Code de la commande publique applicable aux entités publiques	*République française*	**1.4**
CSRD	Directive (UE) 2022/2464 — reporting de durabilité des entreprises	*Parlement européen et Conseil*	**3.2 · 4.3**
ESRS	European Sustainability Reporting Standards — normes de reporting CSRD	*EFRAG / Commission européenne*	**4.3**

5. Référentiels comptables

Cadres comptables nationaux et internationaux applicables aux actifs numériques et aux cryptoactifs.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
IFRS	International Financial Reporting Standards	*IFRS Foundation*	**2.3**
PCG	Plan comptable général	*ANC*	**2.3 · 4.1**
Doctrine ANC	Règlements et avis ANC (notamment ANC 2020-05 et	*ANC*	**2.3**

	2026-02 sur les cryptoactifs)		

6. Cybersécurité, analyse de risques et architecture de confiance

Méthodes d'analyse des risques numériques, référentiels de sécurité et briques d'architecture de confiance.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
EBIOS Risk Manager	Méthode française d'analyse des risques numériques	*ANSSI*	**4.1 · 4.2**
MEHARI	Méthode harmonisée d'analyse des risques	*CLUSIF*	**4.1**
AMDEC / FMEA	Analyse des modes de défaillance, de leurs effets et de leur criticité	*Méthode industrielle (norme NF EN 60812)*	**1.5 · 4.1**
NIST	Cybersecurity Framework du National Institute of Standards and Technology	*NIST (États-Unis)*	**4.2**
PKI	Public Key Infrastructure — infrastructure à clés publiques	*Standards techniques (X.509, RFC 5280)*	**4.2**
IAM	Identity and Access Management — gestion des identités et des accès	*Bonnes pratiques sectorielles*	**4.2**
DLP	Data Loss Prevention — prévention de la fuite de données	*Bonnes pratiques sectorielles*	**2.3**
SIEM / SOC / MSSP	Supervision (SIEM), centre opérationnel (SOC) et prestataire managé (MSSP)	*Bonnes pratiques sectorielles*	**4.2**

7. Durabilité numérique et écoconception

Référentiels et méthodes d'évaluation de l'empreinte environnementale du numérique, et démarches d'écoconception.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
RGESN	Référentiel général d'écoconception des services numériques	*DINUM / ARCEP / ADEME*	4.3
Green IT	Démarche IT for Green / Green for IT	*Communauté professionnelle (greenit.fr, INR)*	1.1 · 4.3
Bilan Carbone®	Méthode française de comptabilité carbone	*ADEME / ABC*	4.3
ACV	Analyse de cycle de vie — méthodologie ISO 14040/14044	*ISO*	4.3
EcoIndex	Indicateur d'empreinte environnementale d'un service web	*Collectif Conception Numérique Responsable*	4.3
GreenIT Analysis	Outil d'audit d'éco-conception web	*GreenIT.fr*	4.3

8. Modélisation, gestion de projet et qualité

Notations de modélisation, méthodes de pilotage de projet et techniques de qualité logicielle.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
BPMN	Business Process Model and Notation — notation de modélisation des processus	*OMG (Object Management Group)*	1.3 · 1.5 · 2.1
UML	Unified Modeling Language	*OMG*	1.5
ArchiMate	Langage de modélisation d'architecture d'entreprise	*The Open Group*	1.3
MEGA	Outil et méthode d'urbanisation des SI (éditeur français)	*MEGA International*	1.3

Cycle en V	Modèle séquentiel de gestion de projet logiciel	*Méthode classique de génie logiciel*	**1.5**
Scrum	Méthode agile itérative et incrémentale	*Schwaber & Sutherland (Scrum Guide)*	**1.5**
Kanban	Méthode visuelle de gestion de flux	*Toyota / D. Anderson*	**1.5**
DevOps	Démarche d'intégration continue Dev + Ops	*Pratiques sectorielles*	**1.5**
GANTT	Diagramme de planification de projet	*Henry Gantt (1910)*	**1.5**
RACI	Matrice des responsabilités (Responsible, Accountable, Consulted, Informed)	*Méthode classique de management de projet*	**1.5**
MoSCoW	Méthode de priorisation (Must, Should, Could, Won't)	*Méthode DSDM Atern*	**1.5**
SWOT	Analyse stratégique forces/faiblesses/opportunités/menaces	*Méthode de management stratégique*	**1.1 · 3.2**

9. Méthodes économiques et de pilotage

Outils d'évaluation financière, de pilotage par la performance et de modélisation économique.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
ABC	Activity-Based Costing — comptabilité par activités	*Cooper & Kaplan (1988)*	**3.1**
TCO	Total Cost of Ownership — coût total de possession	*Gartner*	**2.3 · 3.1**
CAPEX / OPEX	Capital expenditure / Operational expenditure	*Pratique financière internationale*	**3.1**
ROI / NPV / IRR	Return on Investment, Net Present Value, Internal Rate of Return	*Pratique financière internationale*	**3.1**

VAN / TRI	Valeur actuelle nette / Taux de rendement interne (équivalents francophones)	*Théorie financière*	**2.2 · 3.1**
Business Model Canvas	Modèle de représentation du business model	*Osterwalder & Pigneur (2010)*	**2.2**
Value Proposition Design	Modèle de conception de la proposition de valeur	*Osterwalder et al. (2014)*	**2.2**
OKR / KPI / SMART	Objectifs et indicateurs (Objectives & Key Results, Key Performance Indicators, critères SMART)	*Pratiques managériales*	**2.2 · 3.1**
MTTR / MTBF	Mean Time To Repair / Mean Time Between Failures — indicateurs de maintenance	*Ingénierie de la fiabilité*	**1.5**
Balanced Scorecard	Tableau de bord prospectif	*Kaplan & Norton (1992)*	**1.1 · 3.1**

10. Conduite du changement

Modèles d'accompagnement de la transformation organisationnelle et numérique.

Sigle / Nom court	Intitulé complet	Source/Editeur	Sections
ADKAR	Awareness, Desire, Knowledge, Ability, Reinforcement	*Prosci / Hiatt (2003)*	**4.3**
Modèle Kotter	Les 8 étapes de la conduite du changement	*John Kotter (1996)*	**4.3**

Chapitre 2 MATRICE CROISEE — REFERENTIELS × SECTIONS DU PROGRAMME

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
NEP 240	Audit / déontologie											•		•		
NEP 260	Audit / déontologie													•		
NEP 315	Audit / déontologie											•		•		
NEP 500	Audit / déontologie											•		•		
NEP 9510	Audit / déontologie											•				
Code de déontologie	Audit / déontologie													•		
Code IFAC	Audit / déontologie													•		
ISO 8000	Norme ISO									•						
ISO 9001	Norme ISO					•							•			

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
ISO 14001	Norme ISO												•			•
ISO/IEC 20000	Norme ISO											•				
ISO/IEC 22301	Norme ISO												•			
ISO/IEC 25012	Norme ISO								•							
ISO 26000	Norme ISO															•
ISO/IEC 27001	Norme ISO									•		•	•		•	
ISO/IEC 27701	Norme ISO												•			
ISO 31000	Norme ISO													•		
ISO/IEC 38500	Norme ISO		•									•				
COBIT	Gouvernance SI		•									•				
ITIL	Gouvernance SI		•			•						•				
CMMI	Gouvernance SI		•			•										

Référentiel	Catégorie	Partie 1 – Stratégie SI						Partie 2 – Données			Partie 3 – Outils SI			Partie 4 – Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
IT4IT	Gouvernance SI															•
SDIA	Gouvernance SI															•
Modèle Van Grembergen	Gouvernance SI		•													
Henderson & Venkatraman	Gouvernance SI	•														
SAM	Gouvernance SI	•														
IT Balanced Scorecard	Gouvernance SI	•									•					
Digital Maturity Model	Gouvernance SI		•													
Référentiel CIGREF	Gouvernance SI	•	•													
RGPD	Cadre réglementaire			•					•	•		•		•	•	
NIS 2	Cadre réglementaire			•								•		•	•	
DORA	Cadre réglementaire											•				

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
MiCA	Cadre réglementaire			•								•	•			
AI Act / IA Act	Cadre réglementaire			•										•		
DGA	Cadre réglementaire									•						
DSA	Cadre réglementaire									•						
ePrivacy	Cadre réglementaire									•						
eIDAS / eIDAS 2.0	Cadre réglementaire												•	•	•	
LPM	Cadre réglementaire									•				•	•	
Loi PACTE	Cadre réglementaire												•			
Code des marchés publics	Cadre réglementaire				•											
CSRD	Cadre réglementaire											•				•
ESRS	Cadre réglementaire															•
IFRS	Comptabilité									•						

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
PCG	Comptabilité									•				•		
Doctrine ANC	Comptabilité									•						
EBIOS Risk Manager	Cybersécurité / risques													•	•	
MEHARI	Cybersécurité / risques													•		
AMDEC / FMEA	Cybersécurité / risques					•								•		
NIST	Cybersécurité / risques														•	
PKI	Cybersécurité / risques														•	
IAM	Cybersécurité / risques														•	
DLP	Cybersécurité / risques									•						
SIEM / SOC / MSSP	Cybersécurité / risques														•	

Référentiel	Catégorie	Partie 1 – Stratégie SI						Partie 2 – Données			Partie 3 – Outils SI			Partie 4 – Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
RGESN	Durabilité															•
Green IT	Durabilité	•														•
Bilan Carbone®	Durabilité															•
ACV	Durabilité															•
EcoIndex	Durabilité															•
GreenIT Analysis	Durabilité															•
BPMN	Modélisation / projet			•		•		•								
UML	Modélisation / projet					•										
ArchiMate	Modélisation / projet			•												
MEGA	Modélisation / projet			•												
Cycle en V	Modélisation / projet					•										
Scrum	Modélisation / projet					•										

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
Kanban	Modélisation / projet					•										
DevOps	Modélisation / projet					•										
GANTT	Modélisation / projet					•										
RACI	Modélisation / projet					•										
MoSCoW	Modélisation / projet					•										
SWOT	Modélisation / projet	•										•				
ABC	Économie / pilotage										•					
TCO	Économie / pilotage									•	•					
CAPEX / OPEX	Économie / pilotage										•					
ROI / NPV / IRR	Économie / pilotage										•					
VAN / TRI	Économie / pilotage								•		•					
Business Model Canvas	Économie / pilotage								•							

Référentiel	Catégorie	Partie 1 — Stratégie SI						Partie 2 — Données			Partie 3 — Outils SI			Partie 4 — Sécurité & durabilité		
		1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	4.3
Value Proposition Design	Économie / pilotage								•							
OKR / KPI / SMART	Économie / pilotage								•		•					
MTTR / MTBF	Économie / pilotage					•										
Balanced Scorecard	Économie / pilotage	•									•					
ADKAR	Changement															•
Modèle Kotter	Changement															•

Chapitre 3 NOTES CRITIQUES ET PISTES DE COMPLEMENT

Ces notes pointent les zones où le programme DSCG UE5 pourrait gagner à être complété par des référentiels reconnus, soit pour assurer la cohérence interne de la trame, soit pour aligner la formation avec les standards internationaux des établissements accrédités.

1. L'absence des ISA (International Standards on Auditing)

Le programme cite plusieurs NEP — équivalents français des ISA — mais ne mentionne jamais explicitement le corpus international des International Standards on Auditing produit par l'IAASB (International Auditing and Assurance Standards Board). Or les NEP françaises sont elles-mêmes adaptées des ISA. Pour les candidats DSCG amenés à exercer dans des cabinets internationaux ou des institutions accréditées AACSB/AMBA/EQUIS, la mention des ISA correspondantes (ISA 240 pour la fraude, ISA 315 pour l'environnement et le SI, ISA 500 pour les éléments probants) constituerait un complément utile et conforme aux exigences d'internationalisation des cursus.

Les enseignants peuvent introduire ce complément en présentant systématiquement le binôme NEP/ISA lors des séquences sur l'audit (sections 3.2 et 4.1), en s'appuyant sur le Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements de l'IFAC, accessible librement sur ifac.org.

2. L'absence du référentiel COSO sur le contrôle interne

Le programme aborde abondamment le contrôle interne (NEP 260, NEP 315, fiabilité de l'information) sans jamais citer le référentiel COSO (Committee of Sponsoring Organizations of the Treadway Commission), pourtant standard mondial sur le sujet. Le COSO Internal Control — Integrated Framework (édition 2013) et son complément COSO ERM — Enterprise Risk Management (édition 2017) constituent des cadres conceptuels articulés avec les NEP et les ISA, et servent de référence à la plupart des cabinets de conseil et d'audit pour structurer leurs missions.

L'introduction du COSO en partie 4.1, en complément de NEP 260 et NEP 315, permettrait aux candidats de comprendre comment s'articulent contrôle interne, gestion des risques et reporting financier dans les organisations cotées. Le cube COSO et ses cinq composantes (environnement

de contrôle, évaluation des risques, activités de contrôle, information et communication, pilotage) offrent par ailleurs une grille pédagogique particulièrement opérationnelle pour les études de cas.

3. L'asymétrie sur les méthodes de gestion de projet

La section 1.5 cite explicitement les méthodes agiles (Scrum, Kanban) ainsi que le cycle en V et les méthodes hybrides, mais omet les deux référentiels de gestion de projet les plus diffusés à l'international : le PMBOK Guide du Project Management Institute (PMI), et la méthode PRINCE2 d'AXELOS. Cette omission peut surprendre dans la mesure où le programme insiste sur la posture de pilotage et de conseil, qui mobilise précisément ces référentiels dans les grandes entreprises et les administrations.

Pour rétablir l'équilibre, les enseignants peuvent introduire en section 1.5 un panorama comparatif des principales approches : prédictif (cycle en V, PMBOK, PRINCE2), agile (Scrum, Kanban, SAFe pour l'agilité à l'échelle), hybride. L'objectif n'est pas de former à une méthode particulière mais de développer la capacité du candidat à reconnaître et à évaluer la pertinence d'une méthode au regard du contexte projet.

4. Référentiels secondaires absents mais pertinents

Au-delà des trois absences majeures précédentes, plusieurs référentiels secondaires mériteraient également d'être considérés selon les axes de spécialisation choisis par chaque établissement : TOGAF (The Open Group Architecture Framework) pour l'architecture d'entreprise en complément d'ArchiMate ; le DAMA-DMBOK (Data Management Body of Knowledge) pour la gouvernance des données en partie 2.3, plus complet qu'ISO 8000 et ISO/IEC 25012 pris isolément ; le NIST Cybersecurity Framework dans sa version 2.0 publiée en 2024, qui structure l'approche de la cybersécurité autour de six fonctions (Govern, Identify, Protect, Detect, Respond, Recover) ; le SBTi (Science Based Targets initiative) et le GHG Protocol pour la mesure carbone, complémentaires au Bilan Carbone® français.

Ces compléments restent à l'appréciation des équipes pédagogiques, en fonction des secteurs d'activité ciblés par les cas pratiques et des spécialisations disciplinaires de chaque établissement.

Synthèse pédagogique

Le programme DSCG UE5 dans sa version étendue de septembre 2025 mobilise un corpus dense et cohérent de 84 référentiels distincts répartis sur 15 sous-sections. La densité la plus forte se concentre sans surprise

sur la partie 4 (sécurité et durabilité du SI), suivie par la partie 3 (audit et performance des SI). La partie 2 (organisation des données) présente une forte concentration de cadres réglementaires européens, conformément à l'évolution récente du droit du numérique.

Pour les enseignants comme pour les candidats, cette matrice constitue avant tout un outil d'orientation : elle permet de repérer rapidement quels référentiels mobiliser pour traiter une compétence donnée, et inversement de mesurer la portée transversale d'un référentiel à travers le programme. Elle ne dispense évidemment pas d'une lecture approfondie de chaque source d'autorité — les définitions et exigences précises restent à consulter dans les documents originaux référencés en colonne « Source / Éditeur » du chapitre 1.

ARTICULATION RNCP/PROGRAMME

Cette section articule deux niveaux de référence qui régissent l'enseignement et l'évaluation du DSCG UE5 — Management des Systèmes d'Information : la fiche RNCP40998 publiée par France Compétences le 1er juillet 2025 et applicable depuis le 1er septembre 2025, et la trame pédagogique BO version étendue de septembre 2025 qui constitue la feuille de route opérationnelle des enseignants.

La fiche RNCP40998 inscrit le bloc BC05 — Conseiller une organisation sur le management des systèmes d'information sous la forme de six compétences professionnelles certifiables qui décrivent ce que le titulaire du diplôme doit pouvoir faire dans une situation de travail réelle. La trame pédagogique, elle, déplie ces compétences en quinze sous-sections et environ soixante-cinq verbes d'action, qui correspondent aux savoirs et aux savoir-faire à enseigner pour préparer le candidat à attester ces six compétences.

Cette différence de granularité n'est pas un écart à corriger, mais une articulation à comprendre. Le RNCP relève d'une logique d'employabilité — il dit ce qu'un professionnel doit être capable de faire — alors que la trame pédagogique relève d'une logique d'apprentissage — elle dit ce qui doit être enseigné pour développer cette capacité. Les deux niveaux sont indissociables, et c'est leur articulation qui fonde la qualité d'un dispositif de formation conforme à l'approche par compétences.

Le présent livret se structure en trois temps :

- Une matrice de synthèse présente d'abord la cartographie complète des correspondances.
- Six fiches détaillent ensuite chaque compétence certifiée du bloc BC05 : formulation officielle intégrale, sous-sections rattachées, référentiels mobilisables, compétences détaillées du programme, et trois archétypes de situations professionnelles évaluables.
- Une dernière section propose des pistes opérationnelles pour vos équipes pédagogiques en matière de conception d'études de cas, de calibrage des évaluations et de pilotage de l'approche par compétences.

Les archétypes de situations professionnelles méritent une mention particulière. Ils ne constituent pas des sujets d'examen au sens strict, mais des situations-types représentatives des contextes de travail dans lesquels un titulaire du DSCG sera amené à mobiliser la compétence considérée. Ils sont conçus comme une boussole pour les enseignants qui construisent leurs

études de cas et leurs évaluations en cours d'année — et comme un levier de cohérence avec les attendus du jury national.

Chapitre 1 Matrice de synthese RNCP × Programme

Chaque ligne représente une compétence certifiée du bloc RNCP40998BC05. Les sous-sections du programme apparaissent sous forme de pastilles colorées par partie.

Code	Compétence certifiée RNCP	Sous-sections du programme rattachées
C5.1	Aligner et gouverner	1.1 Élaborer et aligner la stratégie des SI 1.2 Concevoir et piloter la gouvernance des SI 1.3 Diagnostiquer et piloter l'évolution des architectures et de l'urbanisation des SI 2.3 Élaborer et piloter la gouvernance stratégique des données
C5.2	Conduire un projet SI	1.5 Planifier, organiser et conduire des projets de SI 1.6 Mettre en œuvre et piloter la gestion des connaissances au sein du SI
C5.3	Déployer et intégrer	2.1 Concevoir l'organisation des données et assurer leur interopérabilité 2.2 Collecter, traiter, analyser et interpréter des données à des fins décisionnelles 3.1 Concevoir, construire et exploiter des outils de pilotage de la performance
C5.4	Contractualiser et optimiser	1.4 Gérer les relations contractuelles et opérationnelles avec les ESN 3.1 Concevoir, construire et exploiter des outils de pilotage de la performance 3.3 Appréhender les usages et enjeux des technologies blockchain et cryptoactifs
C5.5	Sécuriser et rendre résilient	4.1 Identifier, analyser et gérer les risques liés aux SI 4.2 Concevoir, mettre en œuvre et contrôler une politique de sécurité des SI
C5.6	Auditer et transformer	3.2 Auditer, contrôler et évaluer la performance et la conformité des SI 4.3 Intégrer les enjeux de durabilité et de sobriété numérique dans le management des SI

Chapitre 2 FICHES DETAILLEES PAR COMPETENCE CERTIFIEE

Chaque fiche détaille une compétence du bloc BC05 : formulation officielle, sous-sections couvertes, référentiels mobilisables, compétences détaillées du programme et trois archétypes de situations professionnelles.

1. C5.1 · Aligner et gouverner

1.1. Formulation officielle (RNCP40998BC05)

Participer à la mise en cohérence et à l'alignement d'un système d'information (SI) avec les objectifs stratégiques de l'organisation et assurer la gouvernance opérationnelle des réseaux, applications et données liées aux systèmes d'information.

1.2. Sous-sections du programme couvertes

1.1 Élaborer et aligner la stratégie des SI
1.2 Concevoir et piloter la gouvernance des SI
1.3 Diagnostiquer et piloter l'évolution des architectures et de l'urbanisation des SI
2.3 Élaborer et piloter la gouvernance stratégique des données

1.3. Référentiels et cadres mobilisables

Modèle d'alignement de Henderson & Venkatraman (SAM), IT Balanced Scorecard, COBIT, ITIL, ISO/IEC 38500, MAGNum 2026 (CIGREF/IFACI/ISACA), modèle Van Grembergen, Digital Maturity Model (Deloitte/MIT), notations BPMN/UML/ArchiMate/MEGA, ISO 8000 et ISO/IEC 25012 (qualité des données), RGPD.

1.4. Compétences détaillées du programme à développer

- Identifier les principes d'alignement stratégique entre SI et stratégie métier
- Évaluer les impacts des nouvelles technologies sur la performance organisationnelle
- Appliquer une démarche de planification stratégique du SI (SDSI)
- Décrire et choisir un modèle organisationnel de DSI
- Construire un tableau de bord SI intégrant des critères ESG

- Évaluer la gouvernance SI et la maturité numérique d'une organisation
- Cartographier les SI et accompagner la mise en cohérence inter-organisationnelle
- Piloter la gouvernance de l'information et la gouvernance des données

1.5. Archétypes de situations professionnelles évaluables

1. Audit d'alignement stratégique

Un cabinet d'audit reçoit la mission d'évaluer la cohérence entre la stratégie d'une ETI agro-industrielle et son schéma directeur SI. Le candidat est invité à identifier les leviers et les zones de décrochage en mobilisant le modèle de Henderson & Venkatraman et le référentiel MAGNum 2026, puis à formuler des recommandations argumentées.

2 Refonte de la gouvernance DSI après croissance externe

Une PME en croissance externe vient d'absorber trois entités d'activités complémentaires. La direction sollicite un conseil sur le modèle de DSI à privilégier (centralisé, fédéré, hybride) et la mise en place d'un tableau de bord SI intégrant des indicateurs ESG. Le candidat doit caractériser les options et leurs conséquences.

3. Diagnostic de maturité numérique sectoriel

Un groupement d'intérêt économique du secteur médico-social demande un diagnostic de maturité numérique de ses adhérents en vue d'orienter sa stratégie d'investissement mutualisé. Le candidat construit la grille d'évaluation, anime la collecte, propose une cartographie de maturité et un plan d'investissement priorisé.

2. C5.2 · Conduire un projet SI

2.1. Formulation officielle (RNCP40998BC05)

Accompagner l'élaboration, la mise en œuvre, le déploiement, l'appropriation, la conformité, la maintenance, l'évaluation et l'évolution d'un projet SI tout au long de son cycle de vie.

2.2. Sous-sections du programme couvertes

1.5 Planifier, organiser et conduire des projets de SI
1.6 Mettre en œuvre et piloter la gestion des connaissances au sein du SI

2.3. Référentiels et cadres mobilisables

Cycle en V, méthodes agiles (Scrum, Kanban), méthodes hybrides, DevOps, diagramme de GANTT, matrice RACI, méthode MoSCoW, AMDEC/FMEA, ISO 9001, CMMI, ITIL, indicateurs MTTR et MTBF, knowledge management (Nonaka & Takeuchi).

2.4. Compétences détaillées du programme à développer

- Piloter un projet SI dans toutes ses phases (cadrage, planification, suivi, clôture)
- Accompagner la rédaction d'un cahier des charges fonctionnel et technique
- Identifier et qualifier les risques d'un projet SI (techniques, humains, contractuels)
- Analyser et critiquer un plan qualité projet
- Caractériser les méthodes de maintenance (corrective, adaptative, évolutive, préventive)
- Structurer et animer un dispositif de knowledge management dans une organisation

2.5. Archétypes de situations professionnelles évaluables

1. Projet de remplacement d'ERP en mode hybride

Une coopérative agricole de 800 salariés lance le remplacement de son ERP vieillissant. Le candidat est invité à définir le cahier des charges fonctionnel, justifier le choix d'une approche hybride (cycle en V pour le tronc commun, sprints agiles pour les modules métiers), élaborer le plan qualité projet et hiérarchiser les risques en s'appuyant sur la méthode AMDEC.

2. Décision de fin de vie d'une application critique

Une banque privée doit arbitrer sur le devenir d'une application de gestion de portefeuille en fin de vie (dix ans d'exploitation, dette technique élevée). Le candidat analyse les indicateurs MTTR et MTBF des trois dernières années, évalue les options (refonte, remplacement

par un progiciel, migration SaaS) et formule une recommandation argumentée.

3. Déploiement d'un dispositif de knowledge management

Suite à une vague de départs en retraite, un cabinet d'expertise comptable de taille moyenne décide de structurer son knowledge management. Le candidat conçoit l'architecture du dispositif (cartographie des savoirs critiques, outils, gouvernance), définit les indicateurs de pilotage et anticipe les conditions d'appropriation par les équipes.

3. C5.3 · Déployer et intégrer

3.1. Formulation officielle (RNCP40998BC05)

Accompagner le déploiement, la performance, l'évaluation, les fonctionnalités, les niveaux d'externalisation et d'intégration des systèmes d'entreprise.

3.2. Sous-sections du programme couvertes

2.1 Concevoir l'organisation des données et assurer leur interopérabilité
2.2 Collecter, traiter, analyser et interpréter des données à des fins décisionnelles
3.1 Concevoir, construire et exploiter des outils de pilotage de la performance

3.3. Référentiels et cadres mobilisables

Architectures ERP, PGI, CRM, BI, ETL, EAI, API ; modèles cloud IaaS, PaaS, SaaS ; outils d'analyse Excel avancé et Power BI ; méthodes ABC (Activity-Based Costing) et TCO ; indicateurs CAPEX/OPEX, ROI, NPV ou VAN, IRR ou TRI ; cadre des KPI SMART et Balanced Scorecard ; ISO/IEC 25012 (qualité des données).

3.4. Compétences détaillées du programme à développer

- Apprécier un modèle de données relationnel ou alternatif
- Comprendre l'organisation technique des SI et les principes d'interopérabilité
- Identifier la chaîne de valeur des données et exploiter les données pour la création de valeur

- Appliquer une démarche d'analyse adaptée au business model
- Piloter la performance par les données et utiliser un outil d'analyse (Excel, Power BI)
- Mettre en place un dispositif de contrôle de gestion SI
- Analyser les coûts de la fonction SI (TCO, coûts cachés)

3.5. Archétypes de situations professionnelles évaluables

1. Migration cloud d'un système comptable

Un client souhaite migrer son ERP on-premise vers une solution SaaS. Le candidat évalue les impacts sur l'intégration aux outils RH et CRM existants, calcule le TCO comparé sur cinq ans (CAPEX vs OPEX), identifie les risques d'interopérabilité et de réversibilité, et propose un plan de bascule progressif.

2. Mise en place de la facture électronique

À la veille de l'entrée en vigueur de la réforme, le candidat accompagne un cabinet d'expertise dans la transformation des flux EDI et PDF de ses clients vers le portail public de facturation. Il analyse les impacts sur les processus comptables, qualifie les évolutions du contrôle interne et anticipe les besoins de formation des collaborateurs.

3. Tableau de bord BI multi-sources pour un DAF

Le candidat conçoit un tableau de bord Power BI pour un DAF d'ETI qui agrège des données issues de l'ERP, du SIRH et du CRM. Il définit les KPI pertinents au regard du modèle économique, choisit les représentations graphiques, fixe la fréquence de rafraîchissement et anticipe les enjeux de qualité des données.

4. C5.4 · Contractualiser et optimiser

4.1. Formulation officielle (RNCP40998BC05)

Accompagner l'élaboration de contrats de service, des stratégies d'optimisation des coûts et délais et participer à l'actualisation des

indicateurs en proposant des voies d'amélioration et de respect des normes, lois et règlements en vigueur.

4.2. Sous-sections du programme couvertes

1.4 Gérer les relations contractuelles et opérationnelles avec les ESN
3.1 Concevoir, construire et exploiter des outils de pilotage de la performance
3.3 Appréhender les usages et enjeux des technologies blockchain et cryptoactifs

4.3. Référentiels et cadres mobilisables

SLA (Service Level Agreement), TMA, infogérance, contrats SaaS et cloud ; règlement MiCA, loi PACTE, AI Act, RGPD, NIS 2 ; Code des marchés publics ; CIGREF (réversibilité, portabilité et interopérabilité dans les contrats cloud) ; méthodes de chiffrage CAPEX/OPEX et ROI.

4.4. Compétences détaillées du programme à développer

- Identifier les enjeux contractuels avec les ESN (périmètre, propriété, réversibilité)
- Participer à l'élaboration et à la négociation d'un contrat de service
- Suivre la qualité de service via les SLA et indicateurs de performance
- Proposer des voies d'amélioration des indicateurs SI
- Évaluer les opportunités et limites d'un projet blockchain
- Analyser le cadre réglementaire des cryptoactifs (MiCA, NEP, ISO)

4.5. Archétypes de situations professionnelles évaluables

1.Audit d'un contrat d'infogérance arrivant à terme

Une administration publique souhaite renégocier son contrat d'infogérance qui arrive à échéance. Le candidat évalue la qualité du service rendu au regard des SLA, identifie les clauses problématiques (réversibilité incomplète, propriété des données floue, sortie de contrat verrouillée) et propose des KPI de pilotage post-contractualisation, en mobilisant les bonnes pratiques CIGREF.

2. Mise en conformité MiCA d'un prestataire de services sur actifs numériques

Une fintech française qui exerçait sous l'enregistrement PSAN demande un accompagnement à la mise en conformité avec le règlement MiCA. Le candidat analyse les obligations applicables, qualifie le périmètre des activités concernées (CASP, e-money tokens, asset-referenced tokens), identifie les exigences de documentation et propose une feuille de route.

3. Cadrage budgétaire et réglementaire d'un projet d'IA générative

Un comité d'investissement d'une ETI doit arbitrer sur un projet d'IA générative pour la fonction comptable. Le candidat élabore le business case (estimation CAPEX/OPEX, ROI à trois ans, évaluation des coûts cachés), identifie les exigences applicables au titre de l'AI Act et du RGPD, et structure le dispositif de gouvernance.

5. C5.5 · Sécuriser et rendre résilient

5.1. Formulation officielle (RNCP40998BC05)

Participer au choix, à la mise en œuvre et à l'évolution d'une architecture technique et de confiance visant à lutter contre la vulnérabilité interne et externe du SI et à assurer la continuité de l'activité.

5.2. Sous-sections du programme couvertes

4.1 Identifier, analyser et gérer les risques liés aux SI
4.2 Concevoir, mettre en œuvre et contrôler une politique de sécurité des SI

5.3. Référentiels et cadres mobilisables

EBIOS Risk Manager (ANSSI), MEHARI, AMDEC, NIST Cybersecurity Framework ; ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 22301, ISO 31000 ; directives NIS 2, LPM, règlements eIDAS et eIDAS 2.0, RGPD ; briques techniques PKI, IAM, DLP, SIEM, SOC, MSSP ; doctrine ANSSI sur le cloud (SecNumCloud), guides PCA/PRA.

5.4. Compétences détaillées du programme à développer

- Identifier et qualifier les risques liés aux SI (cyber, réglementaires, métiers)
- Analyser l'impact des risques SI sur la production et les états financiers

- Appliquer les cadres réglementaires (NEP, RGPD)
- Contribuer à la fiabilité de l'information produite par le SI
- Élaborer une politique de cybersécurité adaptée aux enjeux de l'organisation
- Appréhender les notions d'architecture de confiance
- Présenter les dispositifs de surveillance (IAM, PCA/PRA, SIEM/SOC)
- Évaluer les responsabilités dans la gestion des SI critiques

5.5. Archétypes de situations professionnelles évaluables

1. Cartographie des risques cyber d'une PME industrielle

Suite à une attaque par rançongiciel survenue chez un concurrent direct, le dirigeant d'une PME industrielle de 200 salariés demande une cartographie des risques cyber. Le candidat applique la méthode EBIOS Risk Manager, identifie les actifs critiques de l'organisation, qualifie les sources de menace et formule cinq mesures de remédiation prioritaires assorties d'un calendrier.

2 Mise à jour du PCA d'une clinique privée

Une clinique privée doit mettre à jour son plan de continuité d'activité suite à une mise en demeure de l'ARS. Le candidat identifie les processus métiers critiques en mobilisant la norme ISO 22301, définit les RTO et RPO acceptables par processus, conçoit le dispositif de reprise et anticipe la gouvernance de crise en cas d'incident majeur.

3 Mise en conformité NIS 2 d'une ETI logistique

Une ETI logistique relevant désormais du périmètre NIS 2 sollicite un accompagnement à la mise en conformité. Le candidat inventorie les obligations applicables (gouvernance cyber, gestion des risques, chaîne d'approvisionnement), structure la chaîne de notification d'incident vers l'ANSSI et propose un plan d'action chiffré sur dix-huit mois.

6. C5.6 · Auditer et transformer

6.1. Formulation officielle (RNCP40998BC05)

Participer à l'élaboration de la documentation et à la mise en œuvre d'un audit du SI afin d'accompagner la direction dans la conception et le déploiement de sa stratégie de transformation numérique.

6.2. Sous-sections du programme couvertes

3.2 Auditer, contrôler et évaluer la performance et la conformité des SI
4.3 Intégrer les enjeux de durabilité et de sobriété numérique dans le management des SI

6.3. Référentiels et cadres mobilisables

Normes d'exercice professionnel NEP 240, 260, 315, 500 et 9510 ; référentiels COBIT, ITIL, ISO/IEC 38500 ; directive CSRD et normes ESRS ; ISO 26000, RGESN, méthodologies Green IT, Bilan Carbone, ACV, EcoIndex, GreenIT Analysis ; modèles de conduite du changement ADKAR et Kotter ; cadres IT4IT et SDIA pour la durabilité stratégique.

6.4. Compétences détaillées du programme à développer

- Réaliser un audit des processus SI (gestion des accès, sauvegardes, PCA/PRA, dématérialisation)
- Porter un regard critique sur la gouvernance SI
- Rédiger une note de synthèse ou un diagnostic d'audit
- Assurer une veille sur les cadres réglementaires (CSRD, ESRS)
- Intégrer les enjeux RSE dans la gouvernance SI
- Appliquer les pratiques Green IT dans les processus SI
- Mesurer l'impact environnemental des SI
- Accompagner la transformation numérique responsable
- Intégrer la durabilité dans la stratégie SI

6.5. Archétypes de situations professionnelles évaluables

1. Audit du SI dans le cadre de la mission de CAC

Un commissaire aux comptes prépare son audit annuel d'une ETI cotée. Le candidat définit le périmètre SI à auditer en application de la NEP 315, identifie les éléments probants à collecter au titre de la NEP 500, formalise les constats et le rapport au comité d'audit

conformément à la NEP 260, et anticipe les diligences spécifiques liées à la NEP 9510.

2. Bilan carbone numérique et plan de réduction

Une banque mutualiste prépare son rapport CSRD et doit publier ses indicateurs ESRS E1 sur le climat. Le candidat évalue l'empreinte carbone du SI (datacenters, terminaux, écoconception logicielle, usages collaborateurs), mobilise les méthodes Bilan Carbone et ACV, et formalise un plan d'action chiffré aligné sur le référentiel RGESN.

3. Pilotage stratégique de la transformation numérique responsable

Le comité exécutif d'une ETI veut accélérer sa transformation numérique tout en intégrant les contraintes ESG. Le candidat propose un schéma directeur pluriannuel intégrant les principes Green IT, mobilise les modèles de conduite du changement (Kotter pour la dimension stratégique, ADKAR pour l'accompagnement individuel) et trace une trajectoire de durabilité conforme aux exigences CSRD/ESRS.

Chapitre 3 PISTES OPERATIONNELLES POUR LES EQUIPES PEDAGOGIQUES

Cette section propose quatre pistes concrètes pour traduire l'articulation RNCP × programme dans le pilotage pédagogique d'une équipe d'enseignants. Elles s'inspirent des bonnes pratiques observées dans les établissements accrédités AACSB, AMBA et EQUIS, où l'approche par compétences est devenue le standard de référence.

- **Cartographier les enseignants par compétence certifiée**

Plutôt que de répartir les enseignants par sous-section du programme, l'équipe gagne à les cartographier par compétence RNCP. Cela permet de constituer six équipes-pivots, chacune responsable de l'enseignement et de l'évaluation d'une compétence certifiée. Chaque équipe-pivot intègre les sous-sections rattachées et coordonne les ressources pédagogiques associées. Cette organisation a deux vertus : elle rend l'équipe collectivement responsable d'un livrable certifiable, et elle force les enseignants à dialoguer entre disciplines.

- **Concevoir les évaluations à partir des archétypes de situations**

Les archétypes proposés dans la section 2 servent de matrice pour concevoir les contrôles continus, les examens blancs et les évaluations en cours d'année. La règle est simple : une évaluation cible une ou deux compétences certifiées, mobilise les sous-sections rattachées, et place le candidat dans une situation professionnelle réaliste. L'évaluation cesse d'être une restitution de connaissances pour devenir une démonstration de compétence. Cette logique est par ailleurs celle du jury national, qui calibre les sujets d'examen sur des situations professionnelles complexes mobilisant plusieurs sous-sections.

- **Articuler le programme avec les autres unités d'enseignement**

Le bloc BC05 s'articule naturellement avec d'autres blocs du DSCG. La compétence C5.5 sur la sécurité dialogue avec le BC04 sur l'audit comptable et financier, autour des NEP communes. La compétence C5.6 sur la transformation numérique et la durabilité dialogue avec le BC02 sur le diagnostic financier et extra-financier, autour des reporting CSRD/ESRS. Et la compétence C5.4 sur la contractualisation dialogue avec le BC01 sur le droit des contrats. L'identification de ces ponts inter-blocs ouvre la voie à des études de cas multi-UE qui préparent la posture d'expert-comptable conseiller, qui est le profil de sortie cible de la réforme.

- **Documenter le parcours de l'apprenant et son progrès en compétences**

Pour les établissements inscrits dans une démarche d'accréditation internationale, la traçabilité du développement des compétences est un attendu fort des accréditeurs. Un portfolio numérique par étudiant, structuré autour des six compétences certifiées du BC05, permet de documenter les productions, les feedbacks formatifs et les paliers de maîtrise atteints. Cet outil rend visible le progrès de l'apprenant au-delà de la note d'examen et nourrit le dossier de VAE pour les candidats qui mobilisent cette voie d'accès à la certification.

- **Conclusion**

Ce livret complète le dispositif documentaire de la réforme avec deux livrets antérieurs : le guide pédagogique principal — qui restitue les ressources, les démarches et les cas pratiques pour chacune des quinze sous-sections — et la matrice des référentiels — qui inventorie les quatre-vingt-quatre cadres normatifs mobilisables. La présente articulation RNCP × programme constitue la troisième pièce du dispositif et clôt la trilogie : elle garantit la cohérence entre l'enseignement délivré, les compétences évaluées et les attendus officiels de France Compétences.

Le passage de l'approche par contenus à l'approche par compétences est progressif. Il suppose une transformation des pratiques pédagogiques, des outils d'évaluation et de la gouvernance des équipes. Les trois livrets de la réforme constituent une boîte à outils, pas une norme contraignante : leur appropriation par chaque enseignant et chaque établissement déterminera la qualité des dispositifs de formation et la réussite des candidats au DSCG nouvelle génération.

LIVRET DE CADRAGE PÉDAGOGIQUE

Ce livret regroupe trois schémas synoptiques qui restituent chacun une lecture différente du programme DSCG UE5. Ensemble, ils constituent un dispositif de cadrage utilisable en réunion de rentrée pédagogique pour aligner une équipe d'enseignants autour d'une vision partagée de la trame ministérielle, de son rythme et de ses transversalités. Ils sont conçus pour fonctionner en complémentarité, chacun éclairant une dimension spécifique du pilotage.

- **Trois lectures complémentaires**

Le synoptique vertical présenté en première lecture restitue la séquence pédagogique des 138 heures, depuis l'ancrage stratégique de la partie 1 jusqu'à la consolidation par la sécurité et la durabilité de la partie 4. Il répond à la question du quoi et de la séquence : quels objets enseigner, dans quel ordre. Cette lecture est la plus immédiate et la plus partagée ; c'est elle que vos enseignants reconnaîtront en première intention.

La frise chronologique présentée en deuxième lecture étale les 138 heures sur les 28 semaines d'un calendrier semestriel typique. Elle introduit les jalons d'évaluation, les volumes hebdomadaires moyens et matérialise les ponts pédagogiques inter-parties. Elle répond à la question du quand et du combien : quel rythme, quels points de bascule, quelles évaluations à quel moment. C'est le support privilégié pour discuter de la temporalité avec une équipe.

La vue par compétences transversales présentée en troisième lecture retourne complètement le programme. Elle fait apparaître quatre fils (diagnostic et conseil, pilotage de la performance, audit et conformité, gouvernance et changement), qui correspondent à quatre postures professionnelles attendues du diplômé. Elle répond à la question du quelles postures et quelle cohérence : comment garantir qu'à travers les quatre parties, l'apprenant développe bien les quatre postures professionnelles attendues. C'est l'outil le plus précieux pour les établissements accrédités AACSB, AMBA et EQUIS, pour lesquelles les Assurance of Learning standards exigent précisément la traçabilité des postures à travers le curriculum.

- **Modes d'emploi**

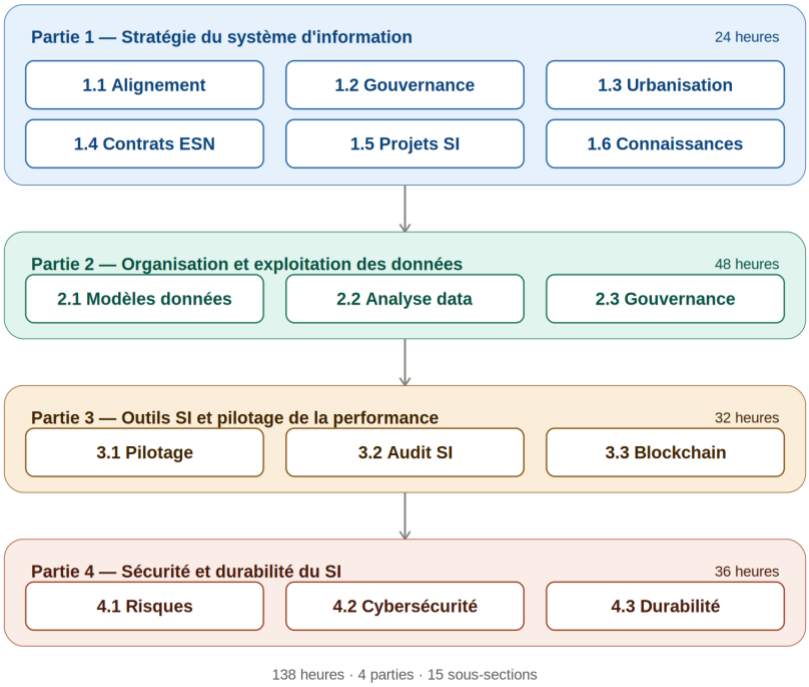
Pour une réunion de rentrée pédagogique, nous recommandons d'enchaîner les trois schémas dans l'ordre du livret. Le synoptique vertical permet à chaque enseignant de se situer dans le programme ; chacun identifie sur

quelle ou quelles cases il intervient. La frise chronologique permet ensuite de discuter le calendrier des évaluations et la cadence des séances. La vue par compétences transversales conclut la séquence en proposant une organisation matricielle de l'équipe : non plus par partie du programme mais par fil transversal.

Pour le pilotage continu en cours d'année, chaque schéma a un usage propre. Le synoptique sert de référence partagée pour identifier les redondances et les manques. La frise sert de tableau de bord temporel pour vérifier l'avancement réel par rapport à la prévision et adapter la cadence si nécessaire. La vue transversale sert de grille de lecture pour les évaluations : chaque sujet d'examen doit pouvoir être positionné sur une ou plusieurs des quatre postures professionnelles, faute de quoi il s'éloigne des attendus du jury national.

1. Synoptique vertical — la séquence pédagogique

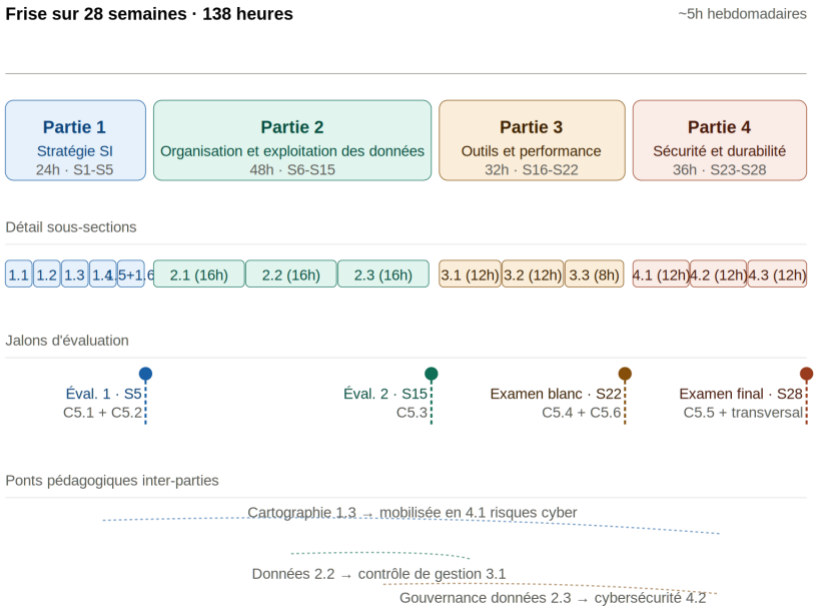
Lecture descendante : de l'ancrage stratégique (partie 1) à la consolidation par la sécurité et la durabilité (partie 4). Les flèches verticales matérialisent une progression cumulative et non une cloison étanche.



Avec 48 heures, la partie 2 sur les données pèse plus du tiers du programme et constitue le centre de gravité de la réforme. La partie 4 (36h) traduit l'attention nouvelle portée à la résilience numérique et à la sobriété environnementale. La partie 1 (24h), la plus courte, joue un rôle de cadrage stratégique sans prétendre à l'exhaustivité.

2. Frise chronologique — le rythme semestriel

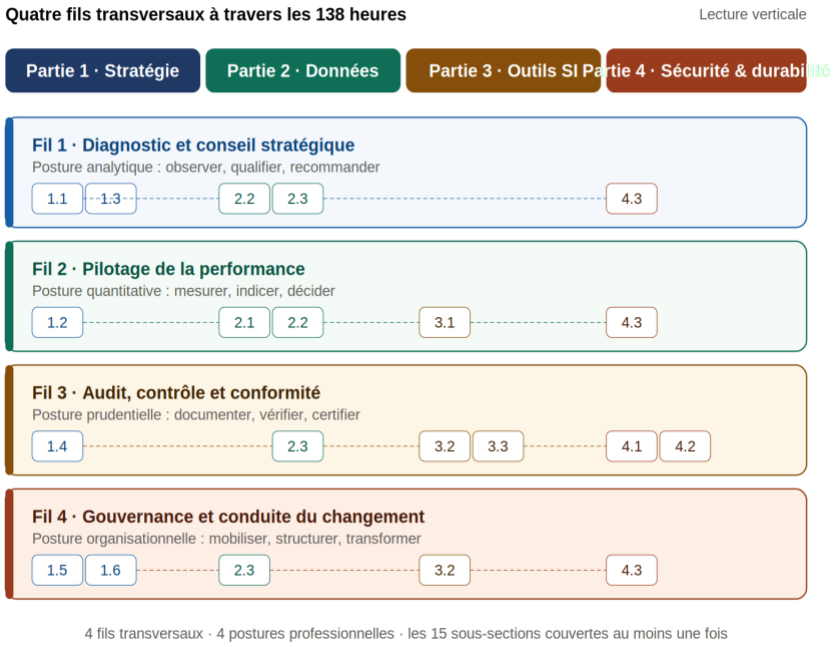
Étalement des 138 heures sur 28 semaines avec quatre jalons d'évaluation et trois ponts pédagogiques inter-parties.



Le rythme moyen est de cinq heures hebdomadaires. La cadence des évaluations vise à éviter l'écueil d'un contrôle trop tardif qui ne permet pas la remédiation : première évaluation en S5 sur les compétences C5.1 et C5.2, deuxième en S15 à la sortie de la partie 2 sur la compétence C5.3, examen blanc en S22 sur C5.4 et C5.6, examen final en S28 sur C5.5 et l'évaluation transversale.

3. Compétences transversales — les quatre postures professionnelles

Lecture verticale du programme par postures professionnelles. Quatre fils traversent les quatre parties et correspondent à quatre identités professionnelles attendues du diplômé.



Cette vue suggère une organisation matricielle des équipes pédagogiques : au lieu de constituer quatre équipes par partie, vous pouvez constituer quatre équipes par posture transversale. Cette organisation améliore la cohérence de l'expérience apprenant et répond aux attendus des accréditations AACSB pour la traçabilité des postures à travers le curriculum.

4. Synthèse — trois lectures, un programme

Les trois schémas ne sont pas concurrents mais complémentaires. Chacun répond à une question différente du pilotage pédagogique et trouve un usage spécifique dans la vie d'une équipe d'enseignants.

Synoptique verticale	Frise chronologique	Compétences transversales
Quoi enseigner et dans quel ordre ?	*Quand et à quel rythme ?*	*Quelles postures professionnelles à développer ?*
Restitue la séquence pédagogique des 138 heures et les 15 sous-sections du programme. Lecture descendante de la stratégie vers la sécurité.	Étale le programme sur 28 semaines avec les jalons d'évaluation et les ponts pédagogiques inter-parties. Lecture chronologique horizontale.	Identifie 4 fils transversaux qui traversent les quatre parties. Chaque fil correspond à une posture professionnelle attendue du diplômé.
Identifier les redondances et les manques. Permettre à chaque enseignant de se situer dans le programme.	Piloter le calendrier des évaluations. Vérifier l'avancement réel par rapport à la prévision.	Constituer une organisation matricielle de l'équipe. Garantir la cohérence des évaluations avec les compétences certifiées.

- **Articulation avec le dispositif documentaire complet**

Ce livret de cadrage prend place dans un dispositif documentaire en quatre pièces. Le Guide pédagogique principal restitue les ressources, les démarches et les cas pratiques pour chacune des quinze sous-sections — c'est l'outil de travail quotidien des enseignants. La Matrice des référentiels inventorie les quatre-vingt-quatre cadres normatifs mobilisables et leur croisement avec les sections du programme — c'est l'outil de cadrage scientifique. L'Articulation RNCP × Programme fait le pont entre la fiche France Compétences et la trame BO en proposant dix-huit archétypes de situations professionnelles évaluables — c'est l'outil de pilotage par compétences. Le présent Livret de cadrage offre une vision synoptique en trois lectures complémentaires — c'est l'outil de réunion d'équipe et de communication interne.

- **Glossaire et acronymes**

Ce glossaire présente les principaux acronymes et termes techniques mobilisés tout au long du guide pédagogique. Il a vocation à constituer un référentiel partagé entre enseignants et candidats au DSCG.

Source. Une partie des entrées de ce glossaire est extraite ou adaptée du CyberDico de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), accessible librement à l'adresse https://cyber.gouv.fr/cyberdico. Ces entrées, signalées par la mention [ANSSI] en fin de définition, sont reproduites sous licence etalab-2.0 (Licence Ouverte v2.0). Les autres entrées correspondent au vocabulaire métier propre au programme DSCG UE5 (gouvernance des SI, finance, comptabilité, droit, durabilité numérique).

Accès local	Attaque avec accès physique au réseau ou à un équipement (Local access). [ANSSI]
AI Act	Règlement européen 2024/1689 sur l'intelligence artificielle.
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité.
ANC	Autorité des normes comptables.
ANSSI	Agence nationale de la sécurité des systèmes d'information.
Attaque par interruption de service (AIS)	Action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu (Denial of Service, DoS). [ANSSI]
Audit	Processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer objectivement pour déterminer dans quelle mesure les exigences d'un référentiel sont satisfaites. [ANSSI]
Authenticité	Propriété d'une information attribuée à son auteur légitime. [ANSSI]
Authentification	Vérification de l'identité dont une entité (personne ou machine) se réclame, par l'apport de la preuve qu'elle s'est vue attribuer un identifiant. [ANSSI]
Authentification forte	Authentification reposant sur un protocole cryptographique (souvent défi-réponse) résistant aux attaques connues. Recommandée par l'ANSSI pour les accès sensibles. [ANSSI]
Backdoor (Porte dérobée)	Accès dissimulé, logiciel ou matériel, qui permet à un utilisateur de se connecter à une machine de manière furtive. [ANSSI]
BI	Business Intelligence — informatique décisionnelle.
BOEN	Bulletin Officiel de l'Éducation Nationale.
Bombe logique	Logiciel malveillant déclenché lorsque certaines conditions sont réunies (date, événement). [ANSSI]
Botnet (Réseau de machines zombies)	Réseau de machines distinctes utilisé à des fins malveillantes (DDoS, pourriels, diffusion de malware) souvent à l'insu des utilisateurs légitimes. [ANSSI]
BSC	Balanced Scorecard — tableau de bord prospectif.
BYOD (Bring Your Own Device)	Utilisation dans un cadre professionnel d'un matériel personnel (smartphone, ordinateur). [ANSSI]
Canular (Hoax)	Information vraie ou fausse, transmise par messagerie ou forum, incitant les destinataires à effectuer des opérations souvent dommageables. [ANSSI]

Cartographie du risque	Représentation visuelle (radar, diagramme de Farmer) des risques issus des activités d'appréciation du risque. [ANSSI]
CDO	Chief Digital Officer ou Chief Data Officer.
CERT/CSIRT	Computer Emergency Response Team / Computer Security Incident Response Team — centre de réponse aux incidents cyber. [ANSSI]
Cheval de Troie (Trojan Horse)	Programme donnant l'impression d'avoir une fonction utile, mais qui possède par ailleurs une fonction cachée et potentiellement malveillante. [ANSSI]
Chiffrement	Transformation cryptographique de données produisant un cryptogramme. [ANSSI]
CIA	Confidentialité, Intégrité, Disponibilité — triade fondamentale de la sécurité de l'information.
CIGREF	Club informatique des grandes entreprises françaises.
Cloud (Infrastructure nuagique)	Modèle permettant un accès aisé, généralement à la demande et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables. [ANSSI]
CNIL	Commission nationale de l'informatique et des libertés.
COBIT	Control Objectives for Information and Related Technologies.
Code malveillant	Tout programme développé dans le but de nuire à ou au moyen d'un système informatique ou d'un réseau (synonyme : maliciel). [ANSSI]
Confiance numérique	Cyberespace de confiance assurant la fiabilité des informations transmises, l'innocuité des services et le respect de la vie privée. [ANSSI]
Confidentialité	Propriété d'une information à laquelle seuls ses destinataires peuvent avoir accès. L'un des trois principes fondamentaux de la sécurité (CIA). [ANSSI]
Cookie	Information stockée par le navigateur lors de la consultation d'un site Internet, permettant au serveur de mémoriser des informations sur l'internaute. [ANSSI]
Crise d'origine cyber	Déstabilisation immédiate et majeure du fonctionnement d'une organisation en raison d'actions malveillantes (rançongiciel, déni de service…) ne pouvant être traitée par les processus habituels. [ANSSI]
Cryptographie	Transformation, au moyen d'un algorithme, d'un message clair en message chiffré, pour assurer disponibilité, confidentialité et intégrité. [ANSSI]
Cryptographie post-quantique	Algorithmes cryptographiques à clé publique conçus pour résister aux attaques d'ordinateurs quantiques de très grande capacité. [ANSSI]
Cryptomonnaie	Monnaie virtuelle permettant aux usagers d'échanger de l'argent de façon anonyme et sans intermédiaire, fonctionnant sur une blockchain. [ANSSI]

CSRD	Corporate Sustainability Reporting Directive (UE 2022/2464).
Cyberattaque	Atteinte à un ou plusieurs systèmes informatiques pour satisfaire des intérêts malveillants. Quatre grandes finalités : appât du gain, déstabilisation, espionnage, sabotage. [ANSSI]
Cybercriminalité	Actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou systèmes d'information comme moyens ou cibles. [ANSSI]
Cyberdéfense	Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les SI jugés essentiels. [ANSSI]
Cyberespace	Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. [ANSSI]
Cybersécurité	État recherché pour un SI lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité. [ANSSI]
DAF	Directeur administratif et financier.
DAMA-DMBOK	Data Management Body of Knowledge (DAMA International).
Darknet	Internet qui nécessite l'utilisation d'un protocole particulier (chiffrement, proxy). [ANSSI]
Déni de service distribué (DDoS)	Action visant à empêcher ou limiter la capacité d'un système à fournir le service attendu, faisant intervenir un réseau de machines compromises. [ANSSI]
DGA	Data Governance Act (UE 2022/868).
DLP	Data Loss Prevention — prévention contre la fuite de données.
DNS (Domain Name System)	Service permettant d'établir une correspondance entre un nom de domaine et une adresse IP. [ANSSI]
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement. [ANSSI]
DORA	Digital Operational Resilience Act (UE 2022/2554).
DPO	Data Protection Officer — délégué à la protection des données.
DSI	Direction des Systèmes d'Information.
EBIOS Risk Manager	Méthode d'analyse de risque française de référence, structurée en cinq ateliers, conforme à ISO 27005:2022. Publiée par l'ANSSI avec le Club EBIOS. [ANSSI]
EFRAG	European Financial Reporting Advisory Group.

Élévation de privilège	Mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement. [ANSSI]
Endiguement (Containment)	Ensemble des actions prises au début d'un incident de sécurité destinées à en contenir l'ampleur. [ANSSI]
Éradication	Recherche et neutralisation des emprises résiduelles ou potentielles de l'attaquant dans le SI. [ANSSI]
ERP	Enterprise Resource Planning — progiciel de gestion intégré.
Escroquerie aux faux ordres de virement (FOVI)	Type d'arnaque visant à manipuler une victime travaillant en entreprise pour qu'elle réalise un virement de fonds non planifié (Business Email Compromise). [ANSSI]
ESG	Environnement, Social, Gouvernance.
ESN	Entreprise de services du numérique.
Espiogiciel (Spyware)	Logiciel collectant et transmettant à des tiers des informations sur l'environnement, à l'insu du propriétaire et de l'utilisateur. [ANSSI]
Espionnage	Type d'attaque consistant pour un attaquant à prendre pied discrètement dans le SI de la victime pour exfiltrer de l'information stratégique. [ANSSI]
ESRS	European Sustainability Reporting Standards.
État de la menace	Caractérisation, sur une période et un périmètre donnés, de la nature et du niveau de risque selon différentes variables (type de menace, modes opératoires, objectifs visés). [ANSSI]
ETL	Extract, Transform, Load.
Exfiltration de données	Vol ou transfert non autorisé des données depuis un terminal ou un réseau. [ANSSI]
Faille (Vulnerability)	Vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement, à la confidentialité ou à l'intégrité des données. [ANSSI]
FEC	Fichier des écritures comptables.
Force-brute (Brute-force)	Technique d'attaque consistant à tester un nombre exhaustif d'authentifiants générés aléatoirement pour le deviner. [ANSSI]
GAGSI	Guide d'audit de la gouvernance du SI (CIGREF/IFACI/ISACA, 2019), prédécesseur de MAGNum 2026.
GED	Gestion électronique de documents.
Gestion de crise cyber	Processus identifiant les impacts potentiels menaçant une organisation et fournissant un cadre pour renforcer la résilience. [ANSSI]

Hachage	Fonction cryptographique transformant une chaîne de caractères de taille quelconque en chaîne de taille fixe. À sens unique et sans collision. [ANSSI]
Hacktivisme	Action d'individus visant à véhiculer des messages et idéologies via des cyberattaques pour amplifier l'écho de leur action. [ANSSI]
Hameçonnage ciblé (Spearphishing)	Attaque reposant sur une usurpation d'identité de l'expéditeur et procédant par ingénierie sociale forte adaptée à la victime. [ANSSI]
Homologation de sécurité	Décision prise par une autorité au sein d'un organisme autorisant le lancement ou le maintien d'un SI. Imposée pour les SI publics, sensibles ou d'importance vitale. [ANSSI]
IA	Intelligence artificielle.
IaaS / PaaS / SaaS	Infrastructure / Platform / Software as a Service — modèles de déploiement cloud.
IFACI	Institut français de l'audit et du contrôle internes.
IFRS	International Financial Reporting Standards.
Incident de sécurité	Événement qualifié compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou des services. [ANSSI]
Indicateur de compromission (IOC)	Combinaison d'informations techniques et contextuelles représentatives d'une manifestation ou tentative de compromission, identifiable par analyse d'un système. [ANSSI]
Infogérance	Prise en charge contractuelle, par un prestataire extérieur, d'une partie ou de la totalité des ressources informatiques d'une entreprise. [ANSSI]
Ingénierie sociale	Manipulation consistant à obtenir un bien ou une information en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes. [ANSSI]
Intégrité	Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime ; et que l'information est correcte et complète. [ANSSI]
Intrusion	Fait, pour une personne ou un objet, de pénétrer dans un espace défini où sa présence n'est pas souhaitée. [ANSSI]
Investigation cyber (Forensic)	Procédé visant à collecter et analyser tout élément technique, fonctionnel ou organisationnel du SI permettant de qualifier une situation suspecte en incident. [ANSSI]
IoT	Internet of Things — Internet des objets.
ISACA	Information Systems Audit and Control Association.
ISO 27001 / 27005	Normes internationales — système de management de la sécurité de l'information / gestion des risques de sécurité de l'information.

ISO 31000	Norme internationale — management du risque.
ITIL	Information Technology Infrastructure Library.
Keylogger	Logiciel ou matériel employé pour capturer ce qu'une personne frappe au clavier. [ANSSI]
KPI	Key Performance Indicator — indicateur clé de performance.
Levée de doute	Ensemble des actions de vérification effectuées pour qualifier un événement survenu sur un système, distinguer un faux-positif d'un incident de sécurité. [ANSSI]
LPM	Loi de programmation militaire.
MAGNum	Modèle de maturité et d'audit de la gouvernance du numérique (CIGREF / IFACI / ISACA France, 2026), successeur du GAGSI.
Maliciel (Malware)	Programme dont le but est de survivre sur un système informatique et d'en parasiter les ressources. [ANSSI]
Man-in-the-middle (Homme-du-milieu)	Catégorie d'attaque où une personne malveillante s'interpose dans un échange de manière dissimulée. [ANSSI]
MCD / MLD	Modèle conceptuel / logique de données.
MDM	Master Data Management — gestion des données de référence.
MEHARI	Méthode harmonisée d'analyse des risques (CLUSIF).
MiCA	Markets in Crypto-Assets (UE 2023/1114).
Mode opératoire d'attaque (MOA)	Signature de l'attaquant, sa façon d'opérer pour cibler et attaquer ses victimes. [ANSSI]
NEP	Normes d'exercice professionnel des commissaires aux comptes (CNCC).
NFT	Non-Fungible Token.
NIS2	Network and Information Security Directive 2 (UE 2022/2555) — vise à renforcer le niveau de cybersécurité des tissus économique et administratif des pays membres de l'UE. [ANSSI]
Nomadisme numérique	Forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI depuis des lieux distants non maîtrisés par l'entité. [ANSSI]
Notification d'incident	Obligation résultant d'un dispositif légal consistant à déclarer un incident de sécurité auprès d'une autorité. [ANSSI]
OIV	Opérateur d'importance vitale — organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation. [ANSSI]

OKR	Objectives and Key Results.
OSE	Opérateur de services essentiels — opérateur tributaire des SI fournissant un service essentiel dont l'interruption aurait un impact significatif. [ANSSI]
PACS	Prestataires d'accompagnement et de conseil en sécurité des SI — référentiel d'exigences ANSSI. [ANSSI]
PAMS	Prestataires d'administration et de maintenance sécurisées — référentiel d'exigences ANSSI. [ANSSI]
Pare-feu (Firewall)	Outil permettant de protéger un ordinateur connecté à un réseau, par filtrage entrant et sortant. [ANSSI]
PASSI	Prestataire d'audit de la sécurité des SI — référentiel d'exigences ANSSI. Couvre audit d'architecture, configuration, code source, tests d'intrusion, audit organisationnel et physique. [ANSSI]
PCA / PRA	Plan de continuité d'activité / Plan de reprise d'activité (ISO 22301).
PCG	Plan comptable général.
PDIS	Prestataire de détection d'incidents de sécurité — référentiel d'exigences ANSSI. [ANSSI]
Phishing (Hameçonnage)	Vol d'identités ou d'informations confidentielles par subterfuge, via simulation d'un système d'authentification légitime. [ANSSI]
Plan de remédiation cyber	Liste des actions à mener pour mettre le SI en conformité avec les objectifs opérationnels de remédiation après incident. [ANSSI]
PMBOK	Project Management Body of Knowledge (PMI).
Point d'eau (Watering hole)	Attaque consistant à piéger un site Internet légitime pour infecter les machines des visiteurs du domaine d'intérêt pour l'attaquant. [ANSSI]
PSAN	Prestataire de services sur actifs numériques.
PSSI	Politique de sécurité du système d'information.
Quishing	Filoutage par code à réponse rapide (QR) ; contraction de QR et phishing — l'attaquant redirige la victime vers une ressource malveillante via un QR code. [ANSSI]
Rançongiciel (Ransomware)	Programme malveillant chiffrant les données du système de la victime pour obtenir le paiement d'une rançon contre le déchiffrement. [ANSSI]
REEN	Loi visant à réduire l'empreinte environnementale du numérique en France (n° 2021-1485).
Remédiation	Projet de reprise de contrôle d'un SI compromis et de rétablissement d'un état de fonctionnement suffisant. [ANSSI]

RGESN	Référentiel général d'écoconception des services numériques.
RGPD	Règlement général sur la protection des données (UE 2016/679) — encadre le traitement des données personnelles dans l'UE. [ANSSI]
RGS	Référentiel général de sécurité — cadre réglementaire visant à limiter la fraude liée à l'utilisation des services numériques de l'administration. [ANSSI]
Rootkit	Logiciel malveillant furtif donnant à un tiers non habilité les droits d'administrateur d'un ordinateur. [ANSSI]
RSSI	Responsable de la sécurité des systèmes d'information.
Sabotage	Opération consistant à conduire une attaque génératrice de dommages sur le SI de la victime, pouvant aller jusqu'à le rendre inopérant. [ANSSI]
SAM	Strategic Alignment Model (Henderson et Venkatraman).
SecNumCloud	Référentiel d'exigences ANSSI pour les prestataires de services d'informatique en nuage (qualification SaaS, PaaS, IaaS). [ANSSI]
Shadow IT	SI réalisés et mis en œuvre au sein d'organisations sans l'approbation de la DSI. [ANSSI]
SI	Système d'information.
SIAD	Système interactif d'aide à la décision.
SIIV	Système d'information d'importance vitale — systèmes pour lesquels l'atteinte à la sécurité diminuerait fortement le potentiel économique ou la sécurité de la Nation. [ANSSI]
SMSI	Système de management de la sécurité de l'information.
Spam (Pourriel)	Tout courrier électronique non sollicité par le destinataire, souvent envoyé simultanément à un grand nombre d'adresses. [ANSSI]
Supply chain attack	Attaque consistant à compromettre un tiers (fournisseur de logiciels, prestataire) afin de cibler la victime finale. Peut affecter un secteur entier. [ANSSI]
TCD	Tableau croisé dynamique.
TCO	Total Cost of Ownership — coût total de possession.
Téléchargement furtif (Drive-by download)	Téléchargement de logiciel malveillant qui s'effectue à l'insu de l'internaute lorsqu'il visite un site web piraté. [ANSSI]
TRI	Taux de rendement interne.

Usurpation DNS (DNS spoofing)	Attaque consistant à envoyer une réponse DNS malveillante à la place du serveur DNS interrogé, ou à modifier la réponse légitime (man-in-the-middle). [ANSSI]
VAN	Valeur actuelle nette.
Vecteur d'attaque	Moyen d'accès utilisé par un acteur malveillant pour exploiter les failles de sécurité (pièces jointes, pages Internet, vulnérabilités non corrigées). [ANSSI]
Visa de sécurité	Distinction délivrée par l'ANSSI permettant d'identifier les solutions de sécurité fiables, à l'issue d'une évaluation par des laboratoires agréés. [ANSSI]
VPN	Virtual Private Network — réseau privé virtuel ; interconnexion de réseaux locaux via une technique de tunnel sécurisé. [ANSSI]
Vulnérabilité	Faille de sécurité pouvant affecter un logiciel, un SI ou un composant matériel. Peut servir de porte d'entrée pour des acteurs malveillants. [ANSSI]
Vulnérabilité jour-zéro (Zero-day)	Vulnérabilité n'ayant fait l'objet d'aucune publication ou n'ayant reçu aucun correctif au moment de son exploitation. [ANSSI]
Webshell	Type de fichier malveillant exécuté comme un code par un serveur web, qui permet un accès et un contrôle à distance via une console malveillante. [ANSSI]
XBRL	eXtensible Business Reporting Language — format de communication financière numérique.

5. Bibliographie consolidée

Cette bibliographie consolide les principales ressources mobilisables tout au long du programme. Elle est structurée en sept rubriques thématiques alignées sur les quatre parties du DSCG UE5. Les ouvrages académiques sont signalés en premier dans chaque rubrique, suivis des publications institutionnelles et professionnelles. Les sites de référence figurent à la fin et constituent les portails de veille à privilégier.

5.1. Manuels de référence pour la préparation au DSCG UE5

Les ouvrages suivants couvrent intégralement le programme de l'unité d'enseignement 5. Ils constituent le socle pédagogique de référence pour les enseignants et les candidats.

BILET, J.-F. (2024). DSCG 5 — Management des Systèmes d'Information. Manuel et applications. Paris : Dunod, coll. Expert Sup.

GODÉ, C. & BIDAN, M. (dir.) (2020). Cas en management des systèmes d'information — Études de cas DSCG 5. Caen : EMS Éditions, coll. Études de cas. Recueil de 16 cas corrigés couvrant les six grandes parties du programme MSI ; contributions de R. Affogbolo, P. Baillette, M. Bidan, G. Biot-Paquerot, A. Girard, G. Lairet, S. Michel, entre autres.

VO HA, V. (2024). DSCG 5 — Management des Systèmes d'Information : 7 sujets inédits avec corrigés détaillés. Paris : Dunod, coll. Expert Sup, 328 p.

5.2. Ouvrages académiques de référence en management des SI

Cette rubrique rassemble les ouvrages académiques structurants pour comprendre la discipline et ses cadres théoriques. Elle nourrit la réflexion enseignante au-delà du périmètre strict de l'examen.

DESQ, S., FALLERY, B., REIX, R. & ROWE, F. (2007). Trente ans de recherche en systèmes d'information : histoire d'un champ. Économies et Sociétés, série W, n° 11, p. 25-42. Article de synthèse historique en accès libre sur sietmanagement.fr.

HENDERSON, J. C. & VENKATRAMAN, N. (1993). Strategic alignment : leveraging information technology for transforming organizations. IBM Systems Journal, vol. 32, n° 1, p. 4-16. Article fondateur sur l'alignement stratégique du SI, librement accessible. Référence centrale du chapitre 1.1 du programme.

MISSONIER, S. (2017). Management d'un projet système d'information : principes, techniques, mise en œuvre et outils. Paris : Dunod, 8e édition.

REIX, R., FALLERY, B., KALIKA, M., RICHET, J.-L. & ROWE, F. (2023). Systèmes d'Information et Management. Paris : Vuibert, 8e édition, 512 p. Ouvrage couronné par le prix FNEGE en 2016 pour son édition précédente. Site associé : sietmanagement.fr (170 études de cas, 80 théories en SI, 25 MOOC sélectionnés). ISBN 978-2-311-41220-8.

5.3. Décarbonation, numérique responsable et durabilité des SI

Rubrique stratégique pour la Partie 4 du programme (sécuriser et rendre durable le SI), elle réunit les contributions académiques francophones les plus récentes sur la décarbonation des systèmes d'information.

ADEME & ARCEP (2024). Évaluation de l'impact environnemental du numérique en France et analyse prospective. Paris : ADEME / ARCEP. Étude conjointe quantifiant l'empreinte carbone du secteur numérique et explorant les scénarios à horizon 2030 et 2050. Disponible sur ademe.fr et arcep.fr.

BIOT-PAQUEROT, G., CLAUZEL, A. & RICHÉ, C. (dir.) (2025). Vers un management durable des systèmes d'information ? Éditions Management & Datascience, 311 p., publié avec le soutien de l'AIM. Ouvrage collectif rassemblant une cinquantaine de contributeurs (M. Bidan, S. Carton, M. Duarte, S. Michel, F. Cocula, A. Bugeau, entre autres) ; couvre la sobriété des datacenters, l'écoconception logicielle, les paradoxes du secteur bancaire, les territoires intelligents et les enjeux pédagogiques. ISBN 978-2-9596430-3-3.

BORDAGE, F. (2019). Sobriété numérique : les clés pour agir. Paris : Buchet-Chastel. Ouvrage de référence pour le grand public et les enseignants, complété par les ressources de greenit.fr.

CIGREF (2024). Stratégies Numérique Responsable des grandes organisations : comment passer à l'échelle ? Paris : Cigref. Disponible librement sur cigref.fr/publications.

CIGREF & INSTITUT DU NUMÉRIQUE RESPONSABLE (2025). L'approche low-tech au service de la résilience numérique des grandes organisations. Rapport conjoint, Paris. Disponible librement sur cigref.fr/publications.

GIRARD, A. & DUARTE, M. (coord.) (à paraître). Management des systèmes d'information : accompagner l'entreprise numérique vers la décarbonation. Caen : EMS Éditions. Ouvrage collectif annoncé, prolongement direct des travaux MSI/décarbonation de l'AIM ; Aurélie Girard (IMT Atlantique, LEMNA) et Magalie Duarte (Burgundy School of Business) coordonnent une équipe d'enseignants-chercheurs autour de la transformation des SI dans une trajectoire bas-carbone.

MISSION INTERMINISTÉRIELLE NUMÉRIQUE ÉCO-RESPONSABLE (2024). Référentiel général d'écoconception des services numériques (RGESN). Paris : DINUM / ARCEP / ADEME.

Disponible sur ecoresponsable.numerique.gouv.fr.

5.4. Gouvernance, stratégie et urbanisation des SI

Cadres et référentiels mobilisables dans les Parties 1 et 3 (rôle stratégique du SI, audit des SI). Ces ressources permettent d'articuler stratégie d'entreprise, alignement SI et création de valeur.

AXELOS (2019). ITIL 4 Foundation. London : The Stationery Office. Référentiel de gestion des services informatiques.

CIGREF (2024). Évaluer le retour sur investissement des solutions d'IA générative et agentique. Paris : Cigref. Cadre méthodologique de mesure du ROI de l'IA en entreprise. Disponible sur cigref.fr/publications.

CIGREF (2024). Modèle d'analyse de la valeur pour le numérique. Paris : Cigref. Outil d'aide à l'évaluation de la valeur créée par les investissements numériques. Disponible sur cigref.fr.

CIGREF (2024). Nomenclature des profils métiers du SI — version 2024. Paris : Cigref. 52 fiches de profils métiers actualisées (Product Manager, Data Engineer, etc.). Disponible librement sur cigref.fr.

CIGREF (2024). Rapport d'orientation stratégique 2024 — 5 ambitions : que faire d'ici 2040 ? Paris : Cigref. Disponible sur cigref.fr/publications.

CIGREF (2024). Réversibilité, portabilité et interopérabilité dans les contrats cloud. Paris : Cigref. Cadre contractuel pour limiter la dépendance aux fournisseurs cloud. Disponible sur cigref.fr.

CIGREF (2025). Rapport d'orientation stratégique 2025 — 4 archétypes de la fonction numérique pour 2040. Paris : Cigref. Disponible sur cigref.fr/publications.

GUEX, F. (2014). Système d'information et création de valeur : pour une meilleure gouvernance des SI. Paris : Eyrolles.

ISACA (2019). COBIT 2019 — A Business Framework for the Governance and Management of Enterprise IT. Schaumburg, IL : ISACA. Référentiel international pour la gouvernance des SI, articulé avec ISO 38500.

ISACA, CIGREF & IFACI (2026). MAGNum 2026 — Modèle de maturité et d'audit de la gouvernance du numérique. Paris : Cigref, 202 p. Successeur du GAGSI (2019), structuré autour de 13 vecteurs et 5 niveaux de maturité, accompagné d'un outil tableur d'évaluation. Disponible librement sur cigref.fr.

ORGANISATION INTERNATIONALE DE NORMALISATION (2015). ISO/IEC 38500:2015 — Gouvernance des technologies de l'information par l'entreprise. Genève : ISO. Norme internationale de référence en gouvernance des SI.

5.5. Cybersécurité, risques SI et résilience

Ressources mobilisables dans les sections 2.3 (gouvernance des données et de l'information), 4.1 (risques) et 4.2 (politique de cybersécurité). Les publications de l'ANSSI constituent le socle de référence en France.

AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ — ENISA (2024). ENISA Threat Landscape Report. Athènes : ENISA. Rapport annuel européen sur l'état de la menace cyber. Disponible librement sur enisa.europa.eu.

ANSSI (2017, mis à jour). Guide d'hygiène informatique — 42 mesures pour renforcer la sécurité de son système d'information. Paris : ANSSI. Disponible librement sur cyber.gouv.fr/publications.

ANSSI (2024). La méthode EBIOS Risk Manager — Le guide. Paris : ANSSI, version conforme à ISO 27005:2022. Disponible librement sur cyber.gouv.fr/publications.

ANSSI (2025). CyberDico — Lexique de la cybersécurité. Paris : ANSSI. Glossaire officiel de référence regroupant termes, expressions et sigles du domaine de la cybersécurité avec leurs équivalents anglais. Disponible librement sur cyber.gouv.fr/cyberdico (licence Etalab 2.0).

ANSSI (2025). Guide de l'homologation de sécurité des systèmes d'information. Paris : ANSSI / DINUM, avril 2025. Modèle des trois lignes de maîtrise, classification des SI. Disponible sur cyber.gouv.fr/publications.

ANSSI (2025). Plan stratégique 2025-2027 — Au cœur d'un collectif, pour une Nation cyber-résiliente. Paris : ANSSI. Disponible sur cyber.gouv.fr/publications.

ANSSI (2026). Panorama de la cybermenace 2025. Paris : ANSSI / CERT-FR, mars 2026. Disponible sur cyber.gouv.fr. Référence chiffrée annuelle (1 366 incidents traités, exfiltrations en hausse de 51 %).

CIGREF (2025). Gouvernance de la sécurité numérique : orientation, déploiement et pilotage. Paris : Cigref, en partenariat avec l'ANSSI. Disponible sur cigref.fr/publications.

ORGANISATION INTERNATIONALE DE NORMALISATION (2022). ISO/IEC 27001:2022 — Sécurité de l'information, cybersécurité et protection de la vie privée. Genève : ISO.

PARLEMENT EUROPÉEN ET CONSEIL (2022). Directive (UE) 2022/2555 (NIS 2) sur la cybersécurité dans l'Union. Journal officiel de l'Union européenne. Disponible sur eur-lex.europa.eu.

5.6. Données, IA et cadre réglementaire européen

Rubrique transverse aux Parties 2 et 3 du programme. Elle articule cadre juridique européen (RGPD, Data Act, AI Act, MiCA), gouvernance des données et exploitation décisionnelle.

AUTORITÉ DES NORMES COMPTABLES (2020, mis à jour 2026). Règlements ANC 2020-05 et 2026-02 relatifs au traitement comptable des cryptoactifs. Paris : ANC. Disponibles sur anc.gouv.fr.

CIGREF (2024). Intelligence artificielle : guide à destination des dirigeants. Paris : Cigref. Vision stratégique de l'IA pour les comités exécutifs. Disponible sur cigref.fr.

CIGREF (2025). Guide de mise en œuvre de l'AI Act — Volet gouvernance. Paris : Cigref. Disponible sur cigref.fr/publications.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2024). Guide de la sécurité des données personnelles. Paris : CNIL. Disponible librement sur cnil.fr.

COUR DES COMPTES (2023). Les crypto-actifs : une régulation à renforcer. Paris : Cour des comptes, 165 p. Disponible sur ccomptes.fr.

FRANCE STRATÉGIE (2018). Les enjeux des blockchains. Paris : France Stratégie. Rapport public de référence sur la blockchain et ses usages organisationnels. Disponible sur strategie.gouv.fr.

NONAKA, I. & TAKEUCHI, H. (1997). La connaissance créatrice : la dynamique de l'entreprise apprenante. Bruxelles : De Boeck. Référence fondatrice sur la conversion connaissance tacite/explicite, mobilisable en gouvernance de l'information.

PARLEMENT EUROPÉEN ET CONSEIL (2016). Règlement (UE) 2016/679 — Règlement général sur la protection des données (RGPD). Journal officiel de l'Union européenne, applicable depuis le 25 mai 2018.

PARLEMENT EUROPÉEN ET CONSEIL (2023). Règlement (UE) 2023/1114 sur les marchés de cryptoactifs (MiCA). Journal officiel de l'Union européenne. Disponible sur eur-lex.europa.eu.

PARLEMENT EUROPÉEN ET CONSEIL (2024). Règlement (UE) 2024/1183 sur l'intelligence artificielle (AI Act). Journal officiel de l'Union européenne. Disponible sur eur-lex.europa.eu.

5.7. Sites institutionnels et ressources transversales

Sites à consulter régulièrement pour actualiser les références au gré des évolutions normatives. Ils constituent les portails d'entrée privilégiés pour la veille pédagogique. Ces ressources sont toutes en accès libre.

ademe.fr Agence de la transition écologique. Études, diagnostics et outils sur l'empreinte environnementale du numérique, méthodologie d'analyse de cycle de vie appliquée aux SI.

annales.org/enjeux-numeriques Revue trimestrielle Enjeux numériques des Annales des Mines. Articles de fond gratuits sur les transformations numériques, accessibles en PDF.

arcep.fr Autorité de régulation des communications électroniques et des postes. Baromètres du numérique, rapports sur le numérique soutenable, indicateurs de qualité de service.

cairn.info Plateforme de revues académiques francophones en sciences humaines et sociales. Accès à la Revue Française de Gestion, Systèmes d'Information et Management, Revue Internationale d'Intelligence Économique.

cigref.fr/publications Bibliothèque numérique du Cigref, librement accessible : MAGNum 2026, Nomenclature des profils métiers du SI, rapports d'orientation stratégique, guides AI Act, travaux sur le numérique responsable, Cahiers des Rencontres Numériques de Strasbourg.

cnil.fr Portail de la Commission nationale de l'informatique et des libertés : guides RGPD, fiches DPO, jurisprudence, doctrine sur l'anonymisation, le Data Act et la monétisation des données.

cyber.gouv.fr Portail officiel de l'ANSSI rassemblant guides d'hygiène informatique, méthode EBIOS Risk Manager, panoramas annuels de la cybermenace, recommandations sectorielles, plan stratégique pluriannuel et CyberDico.

ecoinfo.cnrs.fr Groupement de service du CNRS dédié aux impacts environnementaux des TIC. Ressources scientifiques et études de référence sur l'écoconception et la sobriété numérique.

ecoresponsable.numerique.gouv.fr Portail interministériel dédié au numérique éco-responsable : Référentiel général d'écoconception des services numériques (RGESN), feuille de route gouvernementale, ressources pour les administrations et entreprises.

fun-mooc.fr Plateforme universitaire francophone d'enseignement en ligne. Cours certifiants en gouvernance des SI, Big Data, gestion documentaire, cybersécurité, mobilisables en parcours hybride.

greenit.fr Communauté francophone de référence sur le numérique responsable. Articles, baromètres, méthodes et guides sur la sobriété numérique animés par F. Bordage.

hal.science Archive ouverte pluridisciplinaire française. Accès libre à des milliers d'articles, thèses et chapitres d'ouvrages en management des SI, dont les contributions des laboratoires LEMNA, CEREN, CRG, MRM.

ifaci.com Institut français de l'audit et du contrôle internes : publications professionnelles sur l'audit des SI, des données et de la gouvernance numérique, partenaire de MAGNum 2026.

institutnr.org Institut du Numérique Responsable (INR). Référentiel et label NR, formations Numérique Responsable, ressources pour les organisations engagées dans une démarche durable.

management-datascience.org Plateforme de publication académique de l'AIM (Association Information Management). Articles en accès libre et publication des ouvrages collectifs sur le management des SI, la data science et la décarbonation.

messervices.cyber.gouv.fr Espace ANSSI dédié aux ressources opérationnelles : MOOC SecNumacadémie, fiches méthodes EBIOS, guides sectoriels téléchargeables.

sietmanagement.fr Site académique de référence en management des SI, associé à l'ouvrage Reix-Fallery-Kalika-Richet-Rowe (Vuibert, 2023). Propose 170 études de cas indexées, 80 théories en SI, 25 MOOC sélectionnés, un annuaire de livres blancs et plus de 360 pages Wikipédia documentées.

Note. Les ouvrages annoncés comme « à paraître » correspondent à des publications en cours d'édition au moment de la rédaction du présent guide. Leur référencement sera complété dès parution. Les enseignants sont invités à actualiser périodiquement cette bibliographie au gré des publications académiques et institutionnelles, particulièrement vives sur les thématiques de cybersécurité, d'IA générative, d'AI Act et de décarbonation des SI