DSCG – UE 5

Management des Systèmes d'Information – Epreuve écrite

Volume horaire : 140h – 15 ECTS

Objectifs :

L'UE5 a pour objectif de doter les futurs membres de la profession comptable 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 triple perspective de performance, de conformité et de création de valeur. Le programme vise à 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 de ce programme 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.

Structure du programme :
L'UE 5 est structurée en 4 grands blocs thématiques :

- analyser le rôle stratégique du système d'information dans l'organisation (48 heures) ;
- organiser, exploiter et sécuriser les données de l'organisation (36 heures) ;
- mettre en œuvre des outils SI au service de la performance organisationnelle (20 heures) ;
- sécuriser et rendre durable le système d'information (36 heures).

La répartition horaire entre les parties et sous-parties est donnée à titre indicatif.

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 et recherchées du programme de l'UE 5, à tous les niveaux, dans une démarche d'approfondissement**.

Compétences transversales :

Les candidats doivent, en particulier, être en mesure de structurer, optimiser et animer les éléments d'un cahier des charges :

- Aligner les SI avec la stratégie de l'organisation
  - Intégrer les SI dans la stratégie globale pour soutenir les objectifs organisationnels.
- Maîtriser les concepts, outils et techniques
  - Adapter les outils et techniques SI au contexte spécifique, en soutenant les décisions stratégiques et en optimisant les processus de contrôle de gestion.
- Accompagner le client dans son pilotage de la performance globale des SI
  - Utiliser des indicateurs de performance pour une vision globale de la performance des SI.
  - Accompagner le client par rapport à son cahier des charges pour les entreprises de service numérique (ESN).
- Gérer les risques de cybersécurité
  - Identifier et gérer les risques liés à la cybersécurité, mettre en place des mesures de protection et assurer la conformité réglementaire.
- Analyser et communiquer les résultats
  - Analyser des situations complexes, formuler des préconisations et communiquer les résultats de manière structurée, en tenant compte des enjeux technologiques et de cybersécurité.

Compétences professionnelles	Connaissances et savoirs associés	Limites de connaissances et précisions du champ d'étude
Partie 1 – Analyser le rôle stratégique du système d'information dans l'organisation (48 heures)		
1.1 Élaborer et aligner la stratégie des SI (12 heures)		
Définir une stratégie des systèmes d'information alignée sur les objectifs métiers, en intégrant les opportunités offertes par les technologies émergentes	– Principes d'alignement stratégique SI/métier (modèle SAM, chaîne de valeur, etc.) – Méthodologies de planification stratégique du SI – Outils et méthodes de veille technologique et analyse de l'impact des nouvelles technologies sur les modèles économiques	– Ne pas confondre alignement stratégique et simple adéquation technique. – Ne pas se limiter à une veille passive : intégrer l'analyse prospective dans l'évaluation des opportunités SI.
1.2 Concevoir et piloter la gouvernance des SI (10 heures)		
Mettre en œuvre une gouvernance des systèmes d'information intégrant les parties prenantes clés, des indicateurs de performance et des critères de durabilité	– Modèles organisationnels de la DSI (centralisée, décentralisée, bimodale, etc.) – Enjeux relationnels entre DSI, direction générale et directions métiers – Méthodologies d'évaluation de la maturité numérique (CMMI, COBIT, etc.) – Construction et pilotage de tableaux de bord SI intégrant des dimensions ESG (environnementales, sociales, de gouvernance)	– Le pilotage ESG est à comprendre dans une logique d'indicateurs intégrés, non isolés.

1.3 Diagnostiquer et piloter l'évolution des architectures et de l'urbanisation des systèmes d'information (8 heures)		
Concevoir, cartographier et évaluer l'architecture des systèmes d'information dans une logique d'urbanisation cohérente, en intégrant les technologies émergentes (*blockchain*, IA, registres distribués,…)	– Cartographie applicative et fonctionnelle des SI – Urbanisation des SI, interopérabilité et cohérence inter-organisationnelle – Fonctionnement et usages des technologies émergentes : *blockchain*, registres distribués, IA, … – Impacts organisationnels, juridiques et comptables des nouvelles architectures sur la transformation des métiers – Analyse des processus métiers et rôle des architectures SI dans leur rationalisation	– Ne pas réduire l'urbanisation à une vision strictement technique : elle s'inscrit dans une stratégie globale. – En UE 8 du DCG : interopérabilité fonctionnelle et en UE5 du DSCG : urbanisation stratégique et architecturale. – L'usage de l'IA doit notamment être analysé dans ses effets métiers et non uniquement comme outil technique.
1.4 Gérer les relations contractuelles et opérationnelles avec les ESN (6 heures)		
Concevoir, négocier et sécuriser des relations contractuelles avec des prestataires de services numériques (ESN), en tenant compte des enjeux opérationnels et juridiques	– Typologie des contrats de prestation informatique (régie, forfait, infogérance, etc.) : méthodes d'intégration dans la stratégie SI et la gouvernance contractuelle – Cadre juridique applicable : responsabilité, confidentialité, SLA, RGPD – Méthodologie de négociation contractuelle et analyse des risques – Gouvernance de la relation client-prestataire (pilotage de la prestation, indicateurs de suivi, clauses d'audit)	– L'analyse juridique approfondie relève du droit des contrats informatiques et est exclue du programme de l'UE. – Sont également exclues les dimensions éthiques et RSE des relations fournisseurs. – Est aussi exclue la contractualisation dans les marchés publics.

1.5 Planifier, organiser et conduire des projets de systèmes d'information (6 heures)		
Piloter un projet de système d'information, depuis la rédaction du cahier des charges jusqu'à l'analyse des risques et du plan qualité, dans une logique de performance durable	– Méthodologies de gestion de projet (cycle en V, agile, hybride) – Élaboration d'un cahier des charges fonctionnel et technique – Planification des ressources, délais, coûts et qualité – Identification et gestion des risques (maintenance, évolutivité, sécurité) – Mise en œuvre et contrôle du plan qualité	– L'aspect budgétaire détaillé ne relève pas du programme de l'UE. – Les approches DevOps et CI/CD sont mentionnées mais non approfondies. – Le suivi post-déploiement (TMA, support) n'est abordé que dans une perspective de maintenance évolutive et curative.
1.6 Mettre en œuvre et piloter la gestion des connaissances au sein du système d'information (6 heures)		
Mettre en œuvre une stratégie de gestion des connaissances soutenue par les systèmes d'information, en assurant son pilotage, sa gouvernance et son appropriation organisationnelle	– Architecture fonctionnelle des systèmes de *knowledge management* – Méthodes de gouvernance des dispositifs (rôles, responsabilités, indicateurs) – Intégration des outils de KM dans l'environnement SI : GED, intranet, wiki, forums – Leviers d'appropriation et de transformation des pratiques professionnelles	– La gestion des connaissances dépasse la seule numérisation de l'information. – Le pilotage nécessite une approche systémique : outils, processus, culture. – Le lien avec la gestion des compétences (RH) est complémentaire mais distinct.

Partie 2 – Organiser, exploiter et sécuriser les données de l'organisation (36 heures)		
2.1 Concevoir l'organisation des données et assurer leur interopérabilité (14 heures)		
Structurer et organiser les données dans le système d'information afin d'en garantir la cohérence, la qualité, la circulation fluide et l'interopérabilité avec d'autres systèmes	– Modélisation des données (modèles conceptuels, logiques et physiques) – Architectures orientées données (*datawarehouse*, *datalake*, etc.) – Normes et standards d'interopérabilité (XML, API, formats ouverts) – Gouvernance de la donnée : qualité, cycle de vie, dictionnaire de données	– Est exclu l'approfondissement technique des protocoles d'échange. – L'interopérabilité doit être abordée à la fois sur le plan technique et sur le plan organisationnel.
2.2 Collecter, traiter, analyser et interpréter des données à des fins décisionnelles (14 heures)		
Maîtriser l'ensemble de la chaîne de valeur des données pour produire des analyses pertinentes et éclairer la décision stratégique à l'aide d'outils de data visualisation	– Chaîne de traitement des données : collecte, nettoyage, structuration, analyse, restitution – Méthodologies d'analyse de données (descriptive, exploratoire, prédictive) adaptées au *business model* – Outils décisionnels : Excel avancé, Power BI, Tableau, etc. – Représentation visuelle des résultats et formulation de diagnostics argumentés	– Le développement d'algorithmes de *machine learning* n'est pas attendu. – L'usage des outils ne dispense pas d'une lecture critique des corrélations et biais. – L'interprétation doit être reliée à la stratégie globale, non isolée de son contexte.
2.3 Élaborer et piloter la gouvernance stratégique des données (8 heures)		
Mettre en place une gouvernance stratégique de la donnée intégrant les enjeux de qualité, de conformité, de sécurité, de valorisation et de	– Étapes du cycle de vie des données : création, stockage, usage, archivage, suppression	– L'expertise technique des infrastructures (serveurs, réseaux) n'est pas attendue.

cycle de vie des actifs numériques	– Gouvernance de l'information : rôles, responsabilités, référentiels (ex. : DAMA-DMBOK) – Enjeux du *Big Data, cloud computing, datacenters* et souveraineté numérique – Aspects réglementaires (RGPD, archivage légal) et monétisation des données – Notions de valeur, de patrimoine immatériel et de risque lié aux actifs numériques	– La monétisation doit être abordée de façon critique (modèles économiques, éthique). – Le rôle du *Chief Data Officer* et la structuration de la gouvernance sont illustratifs, non normatifs.
Partie 3 – Mettre en œuvre des outils SI au service de la performance organisationnelle (20 heures)		
3.1 Concevoir, construire et exploiter des outils de pilotage de la performance (budgets, indicateurs, tableaux de bord) (8 heures)		
Mettre en œuvre des dispositifs de pilotage de la performance SI, en intégrant une analyse fine des coûts, des indicateurs et des leviers d'optimisation via des tableaux de bord	– Fondamentaux du contrôle de gestion appliqué aux SI – Analyse des coûts directs et indirects : TCO, coûts cachés, ROI des projets SI – Construction et suivi de tableaux de bord SI (KPI, équilibrage performance / risques / coûts) – Revue et amélioration continue des dispositifs de pilotage	– Les méthodes de contrôle budgétaire classiques ne sont pas approfondies dans le programme de cette UE. – Le pilotage stratégique par les indicateurs suppose une capacité de recul critique. – Est exclu le *reporting* réglementaire (ex. DGFIP, ITIL…).
3.2 Auditer, contrôler et évaluer la performance et la conformité des systèmes d'information (8 heures)		
Conduire des missions d'audit et de contrôle des systèmes d'information afin d'évaluer leur performance, leur conformité réglementaire et la qualité de leur gouvernance	– Méthodologies d'audit SI : cartographie des processus, évaluation des risques, contrôles internes – Critères de performance et de conformité : fiabilité, efficacité, sécurité, conformité RGPD, etc. – Techniques de rédaction d'un diagnostic d'audit et d'une note de synthèse	– L'exécution de tests techniques détaillés (pénétration, *stress test*) n'est pas attendue. – La conformité financière et comptable n'est pas traitée dans le programme de l'UE 5. – L'audit SI suppose une approche multidisciplinaire et une posture critique vis-à-vis de la gouvernance.

	– Facteurs de succès et points de vigilance spécifiques à l'audit SI	
3.3 Appréhender les usages et les enjeux des technologies de la *blockchain* et des cryptoactifs (4 heures)		
Évaluer les opportunités, les risques et le cadre réglementaire associés à la mise en œuvre de solutions fondées sur la *blockchain* et les cryptoactifs dans les organisations	– Fonctionnement des technologies de registres distribués (DLT) – Typologie des applications : traçabilité, certification, finance décentralisée, NFT – Cadres réglementaires émergents : règlement MiCA (*Markets in Crypto-Assets*), NEP, normes ISO – Analyse de la valeur ajoutée, des coûts et des limites d'un projet *blockchain*	– L'approche ne nécessite pas de savoir développer une *blockchain* ou un *smart contract*. – La régulation est en évolution rapide, d'où l'importance d'une veille juridique régulière. – Les effets environnementaux et énergétiques doivent être intégrés dans l'analyse.
Partie 4 – Sécuriser et rendre durable le système d'information (36 heures)		
4.1 Identifier, analyser et gérer les risques liés aux systèmes d'information (12 heures)		
Détecter, évaluer et traiter les risques associés aux systèmes d'information, en intégrant les dimensions réglementaires, éthiques et technologiques, y compris les apports de l'IA	– Typologies des risques SI : cybermenaces, défaillances opérationnelles, risques réglementaires et métiers – Méthodes d'analyse d'impact sur les processus, la continuité de service et les états financiers – Référentiels et cadres réglementaires : RGPD, NEP, ISO 27001, etc. – Fiabilisation des systèmes d'information comptables et décisionnels – Apports potentiels de l'intelligence artificielle dans la détection et la prévention des risques	– L'analyse de sécurité technique (pare-feu, antivirus) n'est pas attendue dans le détail. – Le cadre éthique doit être pensé en lien avec la responsabilité sociale de l'organisation. – Une veille réglementaire est indispensable pour maintenir la conformité des pratiques.

4.2 Concevoir, mettre en œuvre et contrôler une politique de sécurité des systèmes d'information (12 heures)		
Définir et piloter une politique de sécurité du SI, en intégrant les enjeux de cybersécurité, de résilience organisationnelle et de gouvernance des systèmes critiques	– Élaboration d'une politique de cybersécurité fondée sur l'analyse des risques – Notions d'architecture de confiance (authentification, chiffrement, segmentation) – Dispositifs de surveillance et de résilience : IAM (*Identity & Access Management*), PCA/PRA (plans de continuité et de reprise d'activité) – Rôles et responsabilités des acteurs dans la gouvernance des systèmes critiques	– La mise en œuvre technique des solutions de cybersécurité n'est pas exigée. – La sécurité doit être envisagée dans une logique systémique (organisationnelle, humaine, juridique). – Le lien avec les normes ISO 27001 et NIS2 peut être mobilisé mais sans entrer dans les certifications.
4.3 Intégrer les enjeux de durabilité et de sobriété numérique dans le management des SI (12 heures)		
Déployer une stratégie SI responsable en intégrant les principes de durabilité, de sobriété numérique et les exigences réglementaires en matière de RSE et de performance environnementale	– Cadres réglementaires : CSRD (*Corporate Sustainability Reporting Directive*), ESRS (*European Sustainability Reporting Standards*) – Gouvernance SI orientée RSE : inclusion, éthique, sobriété – Bonnes pratiques *Green IT* : éco-conception, mutualisation, cycle de vie des équipements – Outils et indicateurs de mesure de l'impact environnemental des SI – Stratégies de transition numérique responsable (*cloud* éthique, *datacenters* verts, réduction de l'empreinte carbone)	– Les normes environnementales techniques (ex. : ISO 14001) sont mobilisées de manière illustrative. – La transformation numérique responsable nécessite une approche transversale et non cloisonnée. – La durabilité doit être intégrée dans la gouvernance globale du SI, et non comme ajout marginal.