DSCG – UE 5
Management des Systèmes d'Information

Volume horaire : 140 heures

La nouvelle version du programme reprend tous les éléments de l'ancienne version du programme, sauf les éléments qui étaient déjà vus en DCG et le seront probablement dans la nouvelle version du 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. Mais plusieurs points sont à noter :

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

Des compétences techniques à développer semblent émerger du référentiel du CNO :

- La capacité à mettre en place des analyses de données
- La capacité à simuler des scenarii
- La capacité à manipuler des données.

On peut proposer d'étendre la formation des étudiants en prévoyant une formation à des compétences en algorithmes pour la manipulation de données, la construction de scenarii et l'analyse de données. Se pose alors la question des outils à retenir et des cas à construire.

Objectifs :

L'UE5 vise à doter les futurs experts-comptables des compétences nécessaires pour comprendre, piloter et sécuriser les systèmes d'information dans un contexte de gestion et de performance organisationnelle. Elle permet d'analyser les enjeux stratégiques liés aux SI, d'accompagner leur évolution et de garantir leur alignement avec les objectifs de l'organisation. Les candidats apprendront à mobiliser des outils et méthodes pour évaluer les risques, optimiser les processus et assurer la gouvernance des SI. Cette approche intègre les dimensions technologique, réglementaire et managériale, essentielles à une gestion efficace et sécurisée des informations.

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 :

- 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.
- Piloter la performance globale des SI
    - Utiliser des indicateurs de performance pour une vision holistique de la performance des SI.
- Gérer les risques cyber
    - 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 spécifiques :

D'une manière générale, seuls les outils et auteurs incontournables sont précisés. D'autres pourront être mobilisés en plus.

Parties	Compétences professionnelles	Compétences RNCP DSCG visées	Parties de l'ancien programme reprises	Connaissances et savoirs associés	Commentaires et limites de connaissances
Partie 1 – Le SI et son environnement (24h) *Cette partie reprend les parties 1 et 2 de la précédente mouture du programme. On retrouve globalement les mêmes thématiques. Il s'agit d'analyser le rôle et la place du SI, de développer les notions suivantes : gouvernance, gestion de projet, alignement stratégique, urbanisation.*					
1.1 Stratégie SI	- Identifier les principes d'alignement stratégique entre SI et stratégie métier - Évaluer les impacts des nouvelles technologies sur la performance - Concevoir un schéma directeur durable et sécurisé - Appliquer une démarche de planification stratégique du SI	- Mettre en œuvre une démarche d'alignement stratégique du SI - Analyser un schéma directeur - Évaluer la contribution du SI à la stratégie organisationnelle	Partie 1 (alignement stratégique, innovation, schéma directeur)	- Contenu et finalité d'un schéma directeur SI - Logique d'alignement stratégique - Technologies émergentes (cloud, IA, etc.) et impacts sur les processus métiers NEP 315, NEP 330, NEP/ISA 402, ISO 27001, ISO 38500, COBIT 2019, ISO 38500	- Intégration progressive des critères ESG et durabilité - Notion de désalignement stratégique à approfondir selon le contexte sectoriel
1.2 Organisation et gouvernance SI	- Décrire les modèles organisationnels de DSI - Analyser les relations entre DSI, DG et directions métiers - Construire un	- Appréhender la gouvernance d'un SI - Analyser les structures décisionnelles SI - Mesurer la maturité	Partie 1 (gouvernance), Partie 2 (tableaux de bord DSI, RSE)	- Organisation d'une DSI, fonctions et acteurs clés (DSI, RSSI) - Tableaux de bord SI, KPI, intégration des critères ESG - Logiques de	- Approfondir les modèles hybrides (PME/ETI) - Nouveaux rôles type DOSI, enjeux d'agilité

	tableau de bord SI intégrant des critères ESG - Évaluer la gouvernance SI et la maturité numérique	numérique d'une organisation		gouvernance numérique (COBIT, ISO 38500) NEP 250, NEP 260, NEP 315, NEP 570, ISO 27001, ITIL 4, ISO 27014, COBIT 2019	
1.3 Urbanisation et évolution du SI	- Participer à l'élaboration d'une cartographie applicative - Accompagner une démarche de mise en cohérence de SI inter-organisationnels - Analyser les processus métiers et organisationnels	- Cartographier les SI - Rationalisation et interopérabilité des SI	1.3	- Évolution des SI, Open Data, BYOD - Cartographie, urbanisation - ITIL, COBIT, ISO 38500, NEP 315, ISA 402, ISO 27001	- Importance de l'interopérabilité
1.4 Organisation des relations avec ESN	- Identifier les enjeux du contrat - Élaboration et négociation du contrat	- Piloter la relation contractuelle SI	4.2	- SLA, ANS, responsabilité juridique - Plan de continuité d'activité	- Lien avec la gestion de projet
1.5 Gestion de projet SI	- Pilotage projet SI - Cahier des charges, cycle de vie, plan qualité	- Piloter projet SI et risques associés	2.2, 2.3, 2.4	- ISO 25010, CMMI, COBIT, ITIL, PRINCE2, PMBOK, ISO 21500, ISO 27005, NEP/ISA 402	- Intégration des risques dans contrats

	- Gestion risques et maintenance				
1.6 Gestion des connaissances	- Outils collaboratifs - Amélioration outils collaboratifs	- Transformation collaborative numérique	2.5	- KM, Text Mining, outils collaboratifs	- Veille sur les outils collaboratifs
Partie 2 – Organisation et analyse des données (36h) *Cette partie reprend des éléments de l'ancien programme sur l'interopérabilité des logiciels et des données. Elle se développe sur deux aspects nouveaux : le management stratégique des données et surtout l'analyse des donnée*					
2.1 Organisation et interopérabilité des données	- Apprécier un modèle de données relationnelles ou alternatives - Identifier les types de données (structurées, semi-structurées, non-structurées) - Comprendre les principes d'interopérabilité et d'interfaçage des SI - Analyser les enjeux des échanges de données (facture électronique, FEC, API)	- Comprendre l'organisation technique des SI - Appréhender les architectures d'échange de données - Garantir la fiabilité des flux inter-systèmes	Partie 3 (bases de données, interopérabilité, échanges)	- Modèle relationnel, NoSQL, XML, API, ETL - Données FEC, architecture de facturation électronique - Middleware, DataWarehouse, SmartLake	- Approfondir la gestion de la qualité des données et la conformité fiscale - Veille sur les évolutions réglementaires de la facture électronique
2.2 Analyse des données	- Identifier la chaîne de valeur des données - Appliquer une démarche d'analyse des données adaptée	- Exploiter les données pour la création de valeur - Piloter la performance par les	Ajout important (partie nouvelle du programme 2024)	- Démarche SIAD, Dataviz (Power BI, Tableau) - Machine Learning, IA prédictive, Text	- Nécessite une initiation à l'analyse de données appliquée - Importance de distinguer les niveaux

	au business model - Utiliser un outil d'analyse (Excel, Power BI, etc.) - Interpréter les résultats d'une analyse pour la décision	données - Présenter un diagnostic basé sur des données chiffrées		Mining - Indicateurs de performance par les données	de traitement et d'interprétation
2.3 Management stratégique et gouvernance des données	- Identifier les étapes du cycle de vie des données - Apprécier les enjeux du Big Data, cloud, datacenter - Mettre en œuvre une gouvernance des données (qualité, sécurité, archivage) - Intégrer les aspects réglementaires et la monétisation des données	- Appréhender les enjeux stratégiques de la donnée - Piloter la gouvernance de l'information - Garantir la conformité et la valeur des actifs numériques	Partie nouvelle (élargissement des questions de données)	- Big Data, Cloud computing, cycle de vie des données - Archivage, datacenter, conformité réglementaire - Monétisation des données, modèle de gouvernance (DAMA-DMBOK)	- Intégration des cadres de conservation selon les exigences légales - Sensibilisation aux risques liés aux mégadonnées (éthique, sécurité)
Partie 3 – SI et performance (32h) *Cette partie reprend les parties suivantes de l'ancien programme : 4 (Gestion de la performance informationnelle) et 6 (Audit du SI).* *Le volume horaire a donc été adapté en conséquence.*					
3.1 Tableaux de bord, budget et indicateurs	- Identifier et évaluer les indicateurs de performance SI - Analyser les coûts de	- Mettre en place un dispositif de contrôle de gestion SI - Construire et suivre	Parties 4.1, 4.3, 4.4 (Gestion de la performance SI)	- TCO, indicateurs de performance et de durabilité - Qualité des services	- Lien à faire avec UE3 (contrôle de gestion) - Approche comparative

	la fonction SI (TCO, coûts cachés) - Proposer des voies d'amélioration des indicateurs - Élaborer un tableau de bord de pilotage SI	un budget SI - Proposer des indicateurs adaptés à la stratégie de l'organisation		SI, modèle ISSM - Tarification interne, budget de la DSI	sectorielle à intégrer selon les cas
3.2 Audit des SI, contrôle et reporting	- Connaître les référentiels d'audit (COBIT, ITIL, NEP, ISO) - Participer à une mission d'audit SI (planification, exécution, synthèse) - Porter un regard critique sur la gouvernance SI - Rédiger une note de synthèse ou un diagnostic d'audit	- Réaliser un audit des processus SI - Identifier les dysfonctionnements et formuler des recommandations - Apprécier la contribution du SI à la maîtrise des risques	Partie 6 (Audit du SI)	- Typologies d'audit : interne, externe, stratégique - Référentiels : NEP, COBIT, ITIL, ISO 27001 - Gouvernance des audits, synthèse et recommandations	- Exemples de missions contextualisées (PME vs GE) - Bien distinguer l'audit SI et l'audit comptable
Partie 4 – Sécurité et durabilité des SI (36h) *Cette partie évolue un peu en allant plus loin dans la sécurité et notamment sur la question de la cybersécurité en suivant en cela les propositions du CNO. L'accent est moins mis que dans la précédente réforme sur la question du RGPD, mais davantage sur les autres cadres règlementaires liés à la gestion du risque.*					
4.1 Approche du risque	- Identifier les risques liés aux SI (cyber, réglementaires, métiers) - Analyser leur impact	- Intégrer la dimension risque dans la gouvernance SI - Assurer la conformité et la traçabilité du SI	Partie 5.1 (risques et sécurité du SI)	- Typologie des risques (cyber, organisationnels, RGPD) - Cadres normatifs :	- Ne pas confondre risques SI et risques projet - Complémentarité avec l'UE1

	sur la production et les états financiers - Appliquer les cadres réglementaires (NEP, RGPD) - Participer à un audit intégrant les SI	- Contribuer à la fiabilité de l'information produite		NEP 315/330, ISO 27001, NIST, ANSSI - Sécurité des accès, données, intégrité	(responsabilités juridiques) - https://cyber.gouv.fr/publications/panorama-de-la-cybermenace-2023 Voir Agence Nationale de Sécurité des Systèmes d'information - ANSSI
4.2 Organisation d'une politique de sécurité	- Élaborer une politique de cybersécurité adaptée aux enjeux - Appréhender les notions d'architecture de confiance - Présenter les dispositifs de surveillance (IAM, PCA/PRA) - Évaluer les responsabilités dans la gestion des SI critiques	- Formaliser les procédures de sécurisation SI - Définir les responsabilités des acteurs - Intégrer la continuité d'activité dans la stratégie SI	Partie 5.2 (sécurité opérationnelle, continuité d'activité)	- IAM, PKI, signature électronique, surveillance - Matrices de risque, PCA/PRA, ISO 31000 - NIST Cybersecurity Framework, EBIOS	- Sensibilisation indispensable au rôle du RSSI - Différencier sécurité préventive, corrective, curative
4.3 Durabilité / numérique responsable	- Assurer une veille sur les cadres réglementaires (CSRD,	- Intégrer les enjeux RSE dans la gouvernance SI	Partie partiellement nouvelle (ajout de la dimension CSRD/ESRS)	- Green IT, empreinte carbone, LCA, ISO 14001	- Intégration des référentiels à actualiser

	ESRS) - Appliquer les pratiques Green IT dans les processus SI - Mesurer l'empreinte carbone d'un SI - Intégrer la durabilité dans la stratégie SI	- Mesurer l'impact environnemental des SI - Accompagner la transformation numérique responsable		- CSRD, ESRS E1-E2, sobriété numérique - Recyclage, éco-conception, communication durable	régulièrement - Nécessité de croiser les approches techniques et stratégiques
Partie 5 – Veille technologique (12h) *Cette partie a vocation à être revue par arrêté chaque année. Elle porte sur des évolutions technologiques très récentes :*					
5.1 Intelligence artificielle (IA)	- Comprendre les principes de fonctionnement d'un modèle d'IA - Identifier les usages métiers de l'IA (automatisation, aide à la décision) - Évaluer les opportunités et limites de l'IA - Appréhender les enjeux éthiques et réglementaires	- Identifier les impacts des technologies émergentes sur les fonctions comptables et de gestion - Intégrer l'IA dans la réflexion stratégique d'une organisation	Partie nouvelle (veille technologique émergente)	- IA faible / forte, modèles d'apprentissage, entraînement - Applications métiers : bots, traitement de texte, prédiction - Enjeux d'éthique, transparence, réglementation	- Préciser les limites actuelles (hallucination, biais, consommation énergétique) - Suivre les normes en évolution (ISO 22739, IA Act) - https://www.cigref.fr/publications - https://cnnumerique.fr/nos-travaux - https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/gestion-

					traitement-et-analyse-des-donnees/ia-generative
5.2 Internet des objets (IoT)	- Comprendre les principes de fonctionnement de l'IoT - Analyser son impact sur les processus comptables et financiers - Planifier des scénarios d'intégration IoT - Évaluer les transformations des modèles d'affaires	- Appréhender les impacts du numérique sur les organisations - Intégrer des capteurs et objets connectés dans les processus métier	Partie nouvelle (prospective numérique appliquée)	- Capteurs, connectivité, API temps réel - Suivi de stocks, facturation automatisée - PIA, sécurité des objets, écosystèmes IoT	- Défis sécuritaires et éthiques spécifiques à l'IoT - Analyse d'impact économique encore exploratoire
5.3 Blockchain et cryptographie	- Comprendre les principes techniques d'une blockchain - Identifier ses usages en audit, traçabilité, finance décentralisée - Évaluer les opportunités et limites d'un projet blockchain - Analyser le cadre réglementaire (MiCA, NEP, ISO)	- Intégrer les technologies de registres distribués dans la réflexion stratégique - Évaluer les impacts organisationnels, comptables et juridiques	Partie nouvelle (technologie émergente, MiCA)	- Fonctionnement d'un registre distribué, tokens, smart contracts - Cas d'usage : audit, traçabilité, identité numérique - Régulation : MiCA, ISO 22739, NEP applicables	- Technologie en évolution rapide, scénarios à contextualiser - Importance du cadre de confiance et de la gouvernance - https://research.theblockchainforgood.org

Remarques d'intégration et de mise en perspective pédagogique :

- UE1 et conformité : obligation de documenter les violations, les études d'impact, les droits des personnes — à croiser avec les obligations du sous-traitant.
- UE1 : Responsabilité juridique – RGPD, sous-traitance, documentation des violations
- UE2 : Risques et finance – cybersécurité curative, PCA, audit des impacts
- UE3 : Contrôle de gestion – indicateurs SI, tableaux de bord
- UE4 : Audit – audit des systèmes d'information et conformité

- DCG UE5 : Vision fonctionnelle → DSCG : vision stratégique et organisationnelle
- Cybersécurité : renforcer les aspects préventifs dans l'UE5, et faire le lien avec les aspects curatifs financiers (UE2).
- RGPD : distinguer clairement les responsabilités DPO (UE5) / responsable de traitement (UE1).
- Veille technologique : appui des rapports de l'ANSSI et de la DGSI (ingérence économique, veille stratégique) et des différentes agences de l'État.