DIPLÔME SUPÉRIEUR DE COMPTABILITÉ ET DE GESTION

UE5 – MANAGEMENT DES SYSTÈMES D'INFORMATION

SESSION 2020

Éléments indicatifs de corrigé

MANAGEMENT DES SYSTÈMES D'INFORMATION

Durée de l'épreuve : 3 heures - coefficient : 1

Les éléments de corrigés sont donnés à titre indicatif. Les réponses à ces questions sont proposées ici successivement en adoptant une posture simple et factuelle. Toutefois, face à la diversité, l'imbrication et à la transversalité même des concepts liés au management des systèmes d'information de gestion, les réponses peuvent adopter différents angles d'attaque, positionnements et argumentaires.

1. Pourquoi la nomination d'un « DPO » pour un cabinet d'expertise comptable est-elle obligatoire ? (1 point)

Pour les experts comptables, la nomination d'un « DPO » est devenue obligatoire car ils sont amenés à manipuler un grand volume de données et souvent des données personnelles très sensibles (liées à la gestion des bulletins de paies par exemple ou aux évolutions de carrière).

2. Pourquoi le législateur donne-t-il la possibilité de mutualiser la fonction de « DPO » entre plusieurs entreprises ? (1 point)

Le « DPO » peut être mutualisé afin de pouvoir mutualiser les coûts salariaux liées à cette fonction et obtenir des économies d'échelle en augmentant le nombre de dossiers à traiter lorsque l'entreprise est de taille modeste

3. Quel est le rôle du « DPO » vis-à-vis de la direction ? (1 point)

Le « DPO » doit assurer le rôle de relais auprès du chef d'entreprise ou auprès du ou des responsable(s) de traitement des données pour les informer sur les obligations du RGPD et pour réduire les risques de non-conformité.
Le « DPO » doit aussi les informer sur les éventuelles sanctions en cas de non-conformité.

4. Dans quelles situations le DPO peut-il procéder à une « Analyse d'Impact centrée sur la protection des données » (AIPD) ? (1 point)

Le « DPO », lorsqu'il estime qu'un traitement ou un ensemble de traitements est susceptible d'engendrer des risques relativement élevés pour les droits et libertés des personnes concernées, peut se référer au RGPD qui préconise explicitement de procéder à une Analyse d'Impact centrée sur la Protection des Données.
Les autorités européennes ont publié un ensemble de lignes directrices qui permettent de distinguer les cas de traitement des données qui nécessitent (ou pas) de déclencher une Analyse d'Impact et cette analyse sera exigée par la CNIL en cas de contrôle

5. Comment envisagez-vous de présenter et de renseigner ce registre ? (1 point)

Il s'agit de noter systématiquement, sur format papier ou numérique, toutes les informations qui peuvent contribuer à détailler la nature, la finalité et les modalités de sécurisation du traitement des données personnelles.

6. Ce registre est-il obligatoire pour le cabinet « CECL20 » ? Vous justifierez votre réponse. (1 point)

Ce registre n'est pas obligatoire pour le cabinet « CECL20 » car il compte moins de 250 employés, mais il parait fortement recommandé, surtout au regard des dysfonctionnements relevés.

7. Quelles sont les informations à communiquer aux employés ? Quelles sont les modalités de recueil du consentement ? (1 point)

Il est nécessaire de les informer de leurs droits concernant le stockage et l'utilisation de ces données personnelles.
Le recueil du consentement explicite des employées est obligatoire avant de relever leur plaque d'immatriculation.

8. Comment mettre en conformité les contrats du cabinet avec ses prestataires et sous-traitants par rapport à la règlementation sur le traitement des données personnelles ? (1 point)

Il s'agit de leur proposer une mise à jour de conformité de l'ensemble des contrats que le cabinet « CECL20 » en cours d'activité avec ses prestataires et ses sous-traitants.
En effet, le RGPD indique clairement que le ou les sous-traitants sont coresponsables des traitements de données personnelles. Un contrat écrit et signé doit préciser l'ensemble des obligations de chaque partie.

9. Comment prévenir les risques « SI » ? Que faire si ces risques se réalisent ? (1 point)

La prévention des risques « SI » suppose d'élaborer des scenarii puis de rédiger, ou de faire rédiger par un cabinet professionnel, un plan de continuité d'activité.
En cas de problème sévère – attaque, fuite, destruction, intrusion, hameçonnage de télétravailleurs, rançonnage de dirigeants, etc. – il mettre à disposition du personnel la procédure de crise (plan de continuité d'activité).
En cas de violation de données à caractère personnel, il faut prévenir la CNIL sous 72 h maximum.

10. Quelles sont les actions de formation des personnels qui pourraient être mises en place et selon quelles modalités ? (0,5 point)

La sensibilisation du personnel à ces risques passe par des actions de formation.
La formation de l'ensemble des collaborateurs sur les enjeux mais aussi sur les obligations et directives du RGPD – même en situation de crise sanitaire et de confinement - fait partie intégrante de la démarche globale de mise en conformité de l'entreprise.
Ces formations peuvent se faire à l'aide de mises en situation à l'occasion de visites sur les différents sites ou en proposant des sessions de formations et de sensibilisations à distance pour ceux qui seraient en situation de télétravail.

11. En cas de mise en place de formation à distance, quelles sont les précautions à prendre ? (0,5 point)

Il faudra faire attention à utiliser une plateforme de visioconférence sécurisée et certifiée – préférer une version payante avec un contrat de service qui propose des garanties sur le stockage des données, la souveraineté, la localisation des datacenters, le traitement des contenus et le chiffrement/cryptage des échanges – car ces formations peuvent être l'occasion de partager des informations sensibles liées à la sécurité du SI du cabinet.

12. Quels sont les obligations liées au RGPD au sein d'un cabinet d'expertise-comptable ? (1 point)

Le cabinet d'experts comptables est responsable du traitement, *data controller,* car il exploite les données personnelles de ses salariés ou celles de ses clients. Sa mission consiste donc à analyser la façon dont toutes les données à caractère personnel manipulées par le cabinet sont collectées,

traitées, stockées, protégées et donc sécurisées. Le cabinet doit ainsi s'assurer que tous les process et usages répondent bien aux critères du RGPD à savoir notamment :

- « recueillir le consentement pour collecter et traiter la donnée » ;
- « minimiser les données » ;
- « habiliter l'accès selon les profils des collaborateurs » ;
- « donner la possibilité de modifier, supprimer, récupérer les données »
- et « satisfaire les conditions légales de stockage ».

13. Quelles sont les solutions informatiques possibles ? vous mettrez en évidence les avantages et les contraintes de chacune des solutions. (1 point)

De nombreuses solutions logicielles dotées de fonctionnalités liées aux droits des personnes (par exemple liées au droit à la portabilité) facilitent le respect de ces exigences.
Le choix de solutions logicielles et d'applications dédiées, posent la question pour les experts comptables de choisir ou non des solutions externalisées (en mode SaaS) et de bien comprendre ce que cela implique :

1. Pour les cabinets qui ont fait le choix de garder en local leurs infrastructures informatiques, le responsable du traitement ou data controller doit s'assurer de la sécurité physique des serveurs : lieux protégés, redondances des machines dans des lieux différents. Il doit également vérifier que toutes les infrastructures – serveurs, laptop, tablettes, smartphones, ordinateurs fixes, etc. – et tous les applicatifs sont équipés d'outils de sécurité type antivirus, anti-malware, pare-feu, etc. Enfin, il doit sensibiliser les collaborateurs aux bonnes pratiques liées à la sécurité des SI en leur présentant par exemple les éventuelles conséquences de laisser une clé USB ou un mot de passe accessible sur un bureau et/ou en les informant des menaces liées à un Internet mal appréhendé (ransomware, phishing, assistant vocal)
2. Pour les cabinets qui ont fait le choix du SaaS, la sécurité des serveurs et applicatifs hébergés doit être assurée par le prestataire infogérant ou par le CSP (cloud service provider) et de nombreux prestataires – notamment situés sur le territoire national – ont mis en place des infrastructures techniques fiables avec une sécurité 24 h/24 et 7 jours/7.

14. Comment mettre en œuvre les obligations liées au RGPD chez les clients d'un cabinet d'expertise-comptable ? Quelles sont les préconisations de l'Ordre des experts-comptables en la matière ? (1 point)

Le cabinet est un sous-traitant, ou data processor, de ses clients. Aussi, le « DPO » du cabinet doit vérifier la façon dont les données de ses clients sont manipulées et traitées.
L'Ordre des experts comptables souligne qu'il faut reconsidérer les contrats entre les cabinets comptables et leurs clients en incluant dans la lettre de mission de nouvelles clauses explicitement dédiées à leur responsabilité dans les traitements des données personnelles.

15. Quelles sont les règles à respecter lors d'une communication par *newsletter* utilisant une *mailing-list* ? (1 point)

La mailing-list et la newsletter doivent respecter les quelques règles suivantes :

1. Indiquer l'identité de la société pour qui le courriel est envoyé,
2. Proposer un moyen simple et gratuit de s'opposer à la réception de nouvelles sollicitations commerciales en prévoyant un lien de désinscription à la fin ou en pied de page tous les couriels,
3. Au tout début de la collecte, préciser, le cas échéant, que l'adresse électronique sera exploitée à des fins de prospection commerciale et le destinataire doit pouvoir s'opposer à cette utilisation

16. Quelles sont les avancées majeures proposées par le nouveau système d'information ? (1 point)

Les réponses doivent être orientées sur les bénéfices de l'intégration autour de l'homogénéité et de la standardisation des données et des processus et autour de l'unicité de la base de données.
Points importants à développer :

- l'importance d'un paramétrage, d'un déploiement, d'une formation et de saisies de données bien effectués avant, pendant et après l 'implémentation de l'ERP
- les gains en termes de rapidité d'accès à une information de gestion bien homogène et bien actualisée donc des gains en termes de réactivité (time to market) et de capacité de réponse aux clients (devis, audit, reporting, dossier partagé, etc.)

17. Comment structurer votre propos et vos séances pour faire passer vos messages dans chacun des deux séminaires (end-user et key-user) ? (2 points)

Structure du plan

1/ tronc commun (1H) centré sur l'intégration du système d'information	
2.1/ spécialisation qui sera centrée sur le travail opérationnel des EU (2H)	2.2/ spécialisation qui sera centrée sur le travail de contrôle et de paramétrage des KU (2H)
3. Conclusion (1H) sur le bien fondé de cette évolution majeure du système d'information	

1) Le tronc commun sera centré sur l'explication de la logique de la migration. Il faudra expliquer le passage d'un système d'information de gestion qui est passé de non intégré à intégré car l'ancien système était devenu obsolète, peu évolutif et trop lent face à un environnement exigeant et agressif. Après un lourd travail d'implémentation aidé par des consultants intégrateurs extérieurs, ce système est donc devenu – grâce à sa base de données unique qui centralise désormais la totalité des données de l'entreprise et à son interopérabilité en temps réel entre tous les modules indispensables au fonctionnement de l'entreprise – à la fois plus réactif et plus vulnérable. C'est toute la complexité et la richesse d'un passage d'un système à base de données multiples à un système – de type ERP – à base de données unique qu'il faut appréhender.

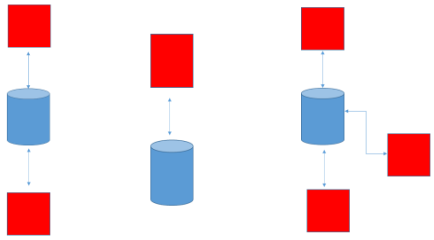
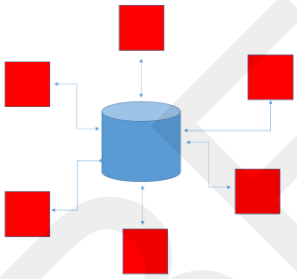
2) Les deux spécialisations proposées :
2.1/ Le premier séminaire centré sur les end-user donc des utilisateurs qui normalement ne sont habilités qu'à saisir et corriger des données et à utiliser des applications fonctionnelles en cohérence immédiate avec leur métier (comptabilité, gestion de la clientèle, achat, fiscalité, trésorerie et recouvrement, paie, etc.).
Ce séminaire devra être centré sur les bonnes pratiques en terme de saisie des données (conformité, standardisation, exactitude, homogénéité, ponctualité, etc.) et de sécurité du poste de travail (mot de passe, confidentialité, etc.). Il faudra insister sur la transversalité du système (ce que vous validez sur votre poste impacte et impacte tout le monde dans un laps de temps quasi immédiat) mais il ne faut pas insister sur la complexité technique du système ni sur son architecture applicative.

2.2/ Le second séminaire s'adresse à des keys user donc à des utilisateurs qui normalement ont déjà été formés d'une part à paramétrer et à maintenir le sous-système fonctionnel dont ils ont la charge et d'autre part – c'est un corollaire – à aider et à accompagner les ends user dans l'exécution de leur tâche et dans leur apprentissage de la logique transverse du système. Ils devront prendre conscience de la transversalité du nouveau système et de leur responsabilité finale sur l'ensemble de leur périmètre fonctionnel notamment en termes de conformité et de sincérité des données mais aussi en termes de plan de continuité d'activité en cas de crise ou de dysfonctionnement (sauvegarde).

3) La conclusion devra motiver tous les utilisateurs et les rassurer sur le fait que l'ERP devrait être finalement une avancée opérationnelle et organisationnelle majeure qui impactera l'ensemble du cabinet et qui le propulsera dans un écosystème plus intégré, plus réactif et plus traçable.

18. Quelle conclusion pourriez-vous proposer lors de ce double séminaire afin de montrer le bien-fondé de cette migration vers un ERP ? (1 point)

Afin de bien aborder cette conclusion destinée à convaincre et à rassurer les deux populations d'utilisateurs après cette lourde migration et les efforts qui sont et seront encore demandés, il est important de s'appuyer sur des données factuelles et illustrées comme par exemple les architectures applicatives bien différentes des deux systèmes analysés :

Système non intégré (avant) : *3 silos (3 DB + 6 Applications)*	*Système intégré (après) :* *1 ERP unique (1 DB + 6 modules)*
	

La conclusion peut souligner que l'architecture modulaire des ERP permet d'être à la fois plus réactifs grâce à la centralisation des données dans l'unique DB et à l'interopérabilité des modules mais aussi plus vulnérables face à une attaque, une malversation ou à de simples anomalies qui auraient pénétrés le système et qui ainsi auraient accès à de très nombreuses informations et applications.

- La responsabilité des end-user est forte car ils doivent veiller à la conformité des données saisies et au respect des processus documentés par l'éditeur concepteur et/ou par l'intégrateur du progiciel intégré.
- Toutefois elle est encore plus forte pour les key-users qui ont la responsabilité du paramétrage pour accompagner au mieux les end-users dans leur tâche quotidienne et de faire fonctionner l'ensemble de leur sous-système fonctionnel (marketing, paie, comptabilité, achat, …) en temps réel et en conformité avec les recommandations de l'intégrateur.

19. Quelles sont les cinq questions que vous aimeriez poser (individuellement et en face à face) à vos employeurs pour évaluer leur niveau d'information en terme de sécurité du « SI » ? (1 point)

Par exemple, afin de bien estimer leurs compétences et leur niveau d'implication à ce sujet, vous pouvez prévoir un questionnaire en face à face, individuel et en temps réel du type :

1) Quelles sont les principales agressions en provenance de l'extérieur ?
2) Quelles sont les principales agressions venues en provenance de l'intérieur ?
3) Lesquelles sont les plus coûteuses en termes d'impact et de dégâts selon vous ?
4) Quels sont les moyens de vous protéger dans chacun de ces deux cas ?
5) Quel est le coût global annuel des mesures de protection de votre entreprise ?

20. Comment pourriez-vous traiter et exploiter leurs réponses afin d'améliorer la sécurité du « SI » du cabinet ? (1 point)

Vous pouvez tenter de quantifier les réponses et de construire un indicateur basique. En fonction des notes que vous attribuerez aux 5 réponses de vos employeurs, vous pourrez évaluer leur niveau (sur une grille de 0 à 10 par exemple) et calculer leur moyenne arithmétique en faisant la somme des 5 notes et en la divisant par 5.

Puis vous leur proposeriez en fonction de leur moyenne (si elle est basse alors le répondant est qualifié de sous-informé, si elle est dans la moyenne des moyennes alors il est correctement informé et si elle est dans la fourchette haute des moyennes alors il sera qualifié de sur-informé) diverses actions à mener qui seront centrées sur les mesures de précautions qualifiées de plutôt actives (logiciel antivirus, sauvegarde des données, plan de continuité, session de formation des utilisateurs, usage de réseaux privés virtuels / virtual private network etc.) et/ou plutôt passives (bonnes pratiques à marteler, modification des mots de passe, déconnexion des ordinateurs, usage précautionneux de la messagerie et des pièces jointes, limiter l'usage des clés usb, vigilance face au à l'hameçonnage (phising), au filoutage et au rançongiciel (ransomware), , etc...).

Vous pourrez aussi leur proposer d'organiser – en invitant des consultants spécialisés en politique de sécurité des SI - des sessions de formation destinées notamment à celles et ceux (cela inclut donc la direction) qui seront amenés à pratiquer le télétravail (identification, extranet/intranet, outils et messageries autorisés/tolérés/non-autorisés, réseau privé virtuel / virtual private network, ordinateur personnel/professionnel, importation/exportation de fichier, etc.). L'objectif de ces séminaires pour CECL20 serait de se mettre en conformité avec la réglementation, les recommandations des services de cyber sécurité et les pratiques de bon sens qui contribuent à protéger les SI des attaques volontaires et/ou involontaires dont d'une part la plupart proviennent de l'intérieur même du système et d'autre part qu'elles sont la plupart du temps largement involontaire et non malveillante mais que les dégâts et les coûts et les délais liés à la remise en fonctionnement du système sont toujours considérables.

Vous pouvez aussi proposer de renouveler cette enquête régulièrement afin d'observer si le niveau d'information des dirigeants évolue favorablement (moyennes de plus en plus élevées) au sein du cabinet ou s'il convient de ne pas relâcher la vigilance et d'accentuer les formations à la sécurité « SI ».