

DIPLÔME SUPÉRIEUR DE COMPTABILITÉ ET DE GESTION

UE5 – MANAGEMENT DES SYSTÈMES D'INFORMATION

SESSION 2020

Durée de l'épreuve : 3 heures

Coefficient : 1

UE5 – MANAGEMENT DES SYSTÈMES D'INFORMATION

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

Document autorisé :

Aucun.

Matériel autorisé :

Aucun.

Document remis au candidat :

Le sujet comporte 6 pages numérotées de 1/6 à 6/6.

Il vous est demandé de vérifier que le sujet est complet dès sa mise à votre disposition.

Le sujet se présente sous la forme de questions.

AVERTISSEMENT

Si le texte du sujet, de ses questions ou de ses annexes, vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement dans votre copie.

SUJET

Le sujet se compose d'une unique étude de cas centrée sur le cabinet « CECL20 ».

Ce cas relate vos dix premières semaines d'expérience professionnelle au sein du cabinet « CECL20 ». Chacune de ces dix semaines – dont certaines furent impactées voire perturbées par la crise de la COVID19, le confinement et le télétravail – vous confronte à une activité ou à une thématique particulière qui est en lien avec les métiers, tâches et responsabilités exercés dans une direction des systèmes d'information.

Le cabinet d'expertise comptable ligérien (CECL20) est une structure assez emblématique de la profession en France avec ses 27 collaborateurs et salariés à temps plein répartis sur ses trois sites (Nantes (15), La Roche-sur-Yon (8) et La Baule (4)). Ce cabinet fonctionne plutôt bien, son turn-over est faible, sa clientèle est fidèle et ses résultats sont bons. Les responsables du cabinet voient toutefois une tendance lourde se profiler, celle du glissement vers les activités de conseil. Pour accompagner cette tendance, et améliorer sa réactivité, le cabinet a modernisé récemment son système d'information. De plus, comme toute la profession, le cabinet se trouve confronté, depuis mai 2018, au déploiement, à la mise en conformité et au respect du Règlement Général sur la Protection des Données à caractère personnel (RGPD). Il se retrouve néanmoins relativement désarmé face à la diversité des aspects qu'il doit aborder et maîtriser à la fois pour lui-même et pour ses clients car – pour rappel - l'article 2 du Règlement général européen sur la protection des données prévoit qu'il s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier »

Ce cabinet vous a donc recruté au regard de vos compétences sur le RGPD et de votre expérience récente de « *data contrôler* ». Cela fait désormais dix semaines que vous évoluez sur son site nantais pour assurer notamment au sein du cabinet la fonction de Délégué à la Protection des Données (DPO) pour accompagner le cabinet vers une protection optimale des données personnelles que « CECL20 » traite à la fois en interne (cabinet) et en externe (clientèle). Vos dix premières semaines comme « DPO » vous ont confronté à de nombreuses thématiques et situations liées au système d'information, aux technologies de l'information, aux données personnelles et au RGPD, aux bonnes pratiques à déployer et à faire respecter parfois au sein même de votre entreprise « CECL20 ». Ces dix semaines sont détaillées ci-après et elles donnent lieu à chaque fois à une ou plusieurs questions.

Semaine 1

Comme vous le savez, pour les cabinets d'expertise comptable, la nomination d'un « DPO » est obligatoire mais, dans certains cas, il peut être mutualisé.

Travail à faire :

1. Pourquoi la nomination d'un « DPO » pour un cabinet d'expertise comptable est-elle obligatoire ? (1 point)
2. Pourquoi le législateur donne-t-il la possibilité de mutualiser la fonction de « DPO » entre plusieurs entreprises ? (1 point)
3. Quel est le rôle du « DPO » vis-à-vis de la direction ? (1 point)

Semaine 2

Après avoir pris connaissance des spécificités du cabinet, et de ses trois sites distants, en matière de collecte, de stockage, de traitement et d'accès visant les données personnelles, mais aussi de la diversité des secteurs d'activité de ses clients répartis sur la région ligérienne, il vous semble que le niveau d'exposition au risque de non-conformité au RGPD n'est pas négligeable et donc qu'une analyse d'impact est opportune.

Travail à faire :

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

Semaine 3 et 4

Après quelques expériences malencontreuses et avoir repéré quelques dysfonctionnements sur le traitement des données personnelles des membres du cabinet (le stockage des plaques d'immatriculations de leurs véhicules sans consentement préalable), vous envisagez de proposer à la direction de « CECL20 » de tenir un registre.

Travail à faire

5. Comment envisagez-vous de présenter et de renseigner ce registre ? (1 point)
6. Ce registre est-il obligatoire pour le cabinet « CECL20 » ? Vous justifiez votre réponse. (1 point)
7. Quelles sont les informations à communiquer aux employés ? Quelles sont les modalités de recueil du consentement ? (1 point)

Semaine 5

Vous continuez vos observations et votre analyse des pratiques du cabinet. Vous avez noté quelques faiblesses, oublis ou imperfections qui peuvent être préjudiciables dans le traitement des contrats avec les prestataires et les sous-traitants

Travail à faire

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

Semaine 6

Vous êtes désormais bien au fait de votre rôle de « DPO », d'autant plus que le cabinet doit faire face à la crise sanitaire liée à la pandémie de la COVID19 qui impacte le cabinet notamment en imposant le télétravail et donc de nouvelles pratiques (visioconférence, partage de fichiers, échanges d'informations, etc.) à un grand nombre de collaborateurs du cabinet. Dès lors, vous devez proposer à votre direction d'envisager un scenario de crise sécuritaire du système d'information qui aurait pour conséquence de perturber gravement l'activité.

Travail à faire

9. Comment prévenir les risques « SI » ? Que faire si ces risques se réalisent ? (1 point)
10. Quelles sont les actions de formation des personnels qui pourraient être mises en place et selon quelles modalités ? (0,5 point)
11. En cas de mise en place de formation à distance, quelles sont les précautions à prendre ? (0,5 point)

Semaine 7

Vos employeurs ont désormais pris conscience de la complexité du dossier qu'ils vous ont confié. Ils apprécient votre professionnalisme, vos capacités d'observation et vos capacités de synthèse face à des questions souvent sensibles. Ils ont noté vos capacités didactiques et pédagogiques quand il s'agit d'aborder les enjeux et obligations liés au RGPD et à son déploiement in situ. Ils aimeraient donc que vous interveniez lors d'une table ronde (environ 10 minutes à l'oral) lors d'un prochain congrès qu'ils organisent à la cité des congrès de Nantes pour les experts comptables du grand ouest afin de montrer les enjeux spécifiques que doivent affronter les congressistes dans leur cabinet. Vous choisissez de structurer votre présentation autour des questions suivantes :

Travail à faire

12. Quels sont les obligations liées au RGPD au sein d'un cabinet d'expertise-comptable ? (1 point)
13. Quelles sont les solutions informatiques possibles ? vous mettrez en évidence les avantages et les contraintes de chacune des solutions. (1 point)
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)

Semaine 8

Vous voulez informer vos collègues et les clients du cabinet de ces nouvelles thématiques et vous envisagez de créer une *mailing-list* et une *newsletter*.

Travail à faire

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

Semaine 9

Au fur et à mesure de votre découverte de l'entreprise « CECL20 » et surtout des usages, appropriations et autres contournements de son système d'information et de gestion par le personnel qui est habilité à l'utiliser, vous avez remarqué que la grande majorité de ces utilisateurs n'a pas pris conscience du processus d'intégration qui vient de se terminer au sein du cabinet.

En effet, l'ancien système n'était pas intégré et était organisé autour de trois silos applicatifs différents et non-interopérables :

- un pour le back office avec une base de données et deux applications,
- un second pour le front office avec une base de données et trois applications
- et enfin, un troisième pour la cybersécurité avec une base de données et une seule application).

Le nouveau système est basé sur le déploiement réussi d'un ERP/PGI proposé en mode *Software as a Service* (SaaS) et hébergé en quasi-totalité sur les datacenters du fournisseur éditeur-leader sur le marché de l'expertise comptable. Cet ERP/PGI est organisé en étoile c'est-à-dire de façon classique. Il dispose de six modules (l'entreprise a acheté et déployé les modules correspondant globalement aux mêmes fonctionnalités que celles dont disposait de l'ancien système) interconnectés à une base de données unique qui est le pivot du système et qui lui permet d'être plus réactif et plus homogène que l'ancien.

Travail à faire

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

Semaine 10

Votre mission de « DPO » touche à sa fin, tout vous semble à présent mis à niveau au sein de « CECL20 ». Toutefois, vous aimeriez faire un sondage auprès de vos employeurs eux même car vous avez un doute sur leur niveau d'information et de vigilance en matière de sécurité de leur propre « SI ». Vous envisagez ensuite de leur dispenser une formation d'une heure tous les ans sur les bonnes pratiques en termes de politique de sécurité de leur propre « SI ».

Travail à faire :

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