1820005

DSCG

SESSION 2018

UE 5 – MANAGEMENT DES SYSTÈMES D'INFORMATION

Éléments indicatifs de corrigé

a supprimé: Bis

a mis en forme : Police :Gras

a supprimé: E

a supprimé: et¶
barème national

a supprimé: ¶
Afin que le jury national puisse se prononcer en toute équité,¶
ce barème doit être respecté par toutes les commissions de correction.¶
¶
¶
¶

a supprimé: ¶
¶
DOCUMENT CONFIDENTIEL¶
AUCUNE DIFFUSION AUTORISÉEE¶
ÀA L'EXCEPTION DES CORRECTEURS¶

a supprimé: CORRIGÉ ET BARÈME INDICATIF

DOSSIER 1 : REMPLACEMENT DU PGI (21 POINTS)

Question 1 : Quels sont les organes à mettre en place pour la gestion de ce projet ? Préciser leur composition et leur rôle respectif.

a supprimé: (3 X 3 points = 9 points)

Le comité de pilotage :

Le comité de pilotage est l'organe directeur de la maîtrise d'ouvrage. Il est présidé par un directeur de projet. Il est composé des représentants opérationnels (responsables métiers et utilisateurs-clés) concernés par le PGI, du responsable informatique, d'experts internes ou externes (intégrateur).

Les attributions du comité de pilotage sont les suivantes :

- lancement du projet caractérisé par les objectifs, les finalités, les critères de qualité et l'arbitrage des moyens à mettre en œuvre,
- définition des choix stratégiques d'architecture et des orientations en matière de sécurité et de droits d'accès,
- accompagner la maîtrise d'ouvrage dans la conduite du changement et sa mise en œuvre intégrant notamment les plans de communication et de formation,
- management du projet correspondant au suivi des échéances, des risques et du contrôle qualité.

Le comité des utilisateurs :

Le comité d'utilisateurs est constitué de tous les utilisateurs représentatifs des domaines d'activité concernés par le projet (achats, commercial, fabrication, comptabilité, contrôle de gestion).

Ses attributions sont les suivantes :

- expression détaillée des besoins et des règles de gestion,
- validation des solutions / maquettes présentées par l'équipe projet,
- participation aux tests du PGI,
- participation aux actions de formation,
- réception définitive du progiciel,
- accompagnement du déploiement. Peut devenir centre de ressources dans la phase post-projet.

Le chef de projet :

Le pilotage du projet est assuré par le chef de projet. Il préside les réunions. Il assure la coordination des différents acteurs et rend compte à la direction de l'avancement du projet. Il est l'interlocuteur de la maîtrise d'ouvrage. Il supervise la réalisation des tests et le recettage. Il valide les supports (documentation, formation).

Le chef de projet doit avoir l'autorité nécessaire pour mener à bien le projet, selon l'ampleur de celui-ci. Ici le projet concerne toute l'entreprise avec des implications organisationnelles. Il est donc nécessaire que le choix du chef de projet traduise un engagement fort de la direction. Il semblerait donc logique que ce soit le DAF, membre du comité de direction, et non le responsable informatique.

Question 2 : Quelles sont les principales conditions de réussite du projet ? (Quatre conditions sont attendues.)

a supprimé: (4 X 1 point = 4 points - Si pas d'argumentation, 0,25 par condition citée.)¶

Conditions de réussite :

- Les objectifs doivent être clairement définis pour permettre de se référer constamment aux raisons qui ont conduit à lancer le projet et prendre des décisions en conséquence ;
- Les équipes projets doivent être organisées avec soin en veillant à mettre en place les contrôles appropriés ;
- Ne pas négliger la dimension humaine du projet qui implique l'animation et la motivation des équipes ;
- Prendre en compte la gestion du changement en intégrant les acteurs concernés dans l'équipe projet et en ayant une communication appropriée ;
- Maîtriser les délais et les coûts, ce qui implique une analyse des risques.

Accepter toute proposition pertinente.

Question 3 : Lors du choix d'un PGI, quels sont les points auxquels l'entreprise doit être attentive ?

a supprimé: CORRIGÉ ET BARÈME INDICATIF

Citer et expliciter quatre points clés.

Points d'attention :

- PGI multilingue, multidevises et multi-référentiel comptable afin de permettre l'entrée de la société suédoise dans le périmètre du groupe Mirlac et une uniformisation des SI afin de bénéficier pleinement des effets de synergie induits par cette opération de croissance externe.
- Coût global du PGI (ou coût total de possession TCO). Ce sont les sommes dues à l'éditeur pour le droit d'utilisation du PGI (généralement en fonction du nombre d'utilisateurs) et, par la suite, pour le maintenir à niveau. Les coûts des mises à jour sont conséquents par rapport à ceux des licences. De plus, il faut ajouter les coûts d'installation (équipe projet, intégrateur, formation…), les éventuels coûts d'adaptation de l'environnement matériel et les coûts cachés (baisse de productivité lors de la mise en œuvre…).
- Adaptabilité du PGI (possibilités de paramétrage) : la souplesse du PGI détermine son degré d'adaptation au contexte de l'entreprise. Un PGI trop rigide impose des contraintes qui nécessitent d'adapter l'entreprise au PGI.
- Complexité du PGI : le paramétrage peut être source de difficultés. Cela peut augmenter considérablement la durée et le coût du projet.
- Expérience et pérennité de l'éditeur : la relation avec l'éditeur s'inscrit dans la durée (mises à jour). Son expérience garantit la pertinence de ses choix. Elle permet aussi d'apprécier sa capacité à durer, ce qui est important car en cas de défaillance, l'entreprise devrait probablement changer de PGI et repartir à zéro avec un autre éditeur. : l'existence d'un grand nombre d'entreprises utilisatrices, en plus de garantir l'expérience de l'éditeur, permet d'envisager des échanges entre utilisateurs (forums, listes de diffusion…) permettant d'accélérer et de capitaliser l'expérience collective.
- Conditions de mise en œuvre : modes d'accès possibles (client lourd, client léger, solution cloud…), ressources nécessaires, aspects juridiques...

Accepter toute proposition pertinente.

Question 4 : Quelles sont les principales difficultés rencontrées lors de la mise en place d'un PGI ? (Quatre difficultés sont attendues.)

Nécessité d'adapter certains processus aux contraintes du progiciel.	L'entreprise doit parfois modifier son organisation afin de s'adapter aux contraintes du progiciel, notamment pour pouvoir utiliser la version et le paramétrage standard. Il faut arbitrer entre impact organisationnel et complexité des paramétrages.
Le projet impacte l'organisation dans son ensemble	Cela implique des risques, au-delà de ceux inhérents à la dimension informatique du projet, en particulier si la gestion du changement est mal appréhendée.
Coûts induits très importants, et souvent sous-estimés.	Il y a de nombreux coûts induits, en termes de temps de travail des personnels, de baisse d'efficacité des services liée à la désorganisation que peut entraîner la mise en place du PGI.
Dépendance vis-à-vis d'un éditeur	Retour en arrière ou changement de PGI difficiles compte tenu de l'importance du projet et de son caractère structurant pour l'entreprise.
Dépendance par rapport aux intégrateurs et aux consultants.	L'intervention d'intégrateurs et de consultants crée des situations d'asymétrie d'information avec des risques au niveau des choix effectués, des coûts, des tensions possibles entre salariés de l'entreprise et salariés extérieurs.

a supprimé: (4 X 1 point = 4 points - Si pas d'argumentation, 0,25 par point d'attention cité.)…

a supprimé: .

a supprimé: (4 X 1 point = 4 points - Si pas d'argumentation, 0,25 par difficulté citée.)…

a mis en forme : Justifié

a mis en forme le tableau

a mis en forme : Justifié

a mis en forme : Justifié

a mis en forme : Justifié

a mis en forme : Justifié

a supprimé: CORRIGÉ ET BARÈME INDICATIF

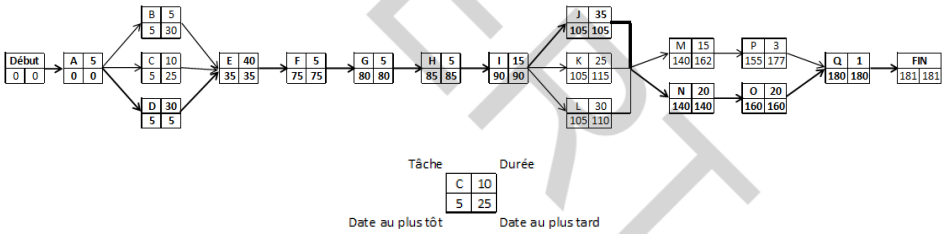
Complexité du paramétrage	Pour être au plus près des processus de l'entreprise, l'installation nécessite une modélisation du fonctionnement de celle-ci, une définition précise des actions et des rôles. Cette étude approfondie peut entraîner un dépassement des délais et des coûts ou un risque de difficultés d'utilisation lors du déploiement.

Accepter toute idée pertinente.

DOSSIER 2 : ORDONNANCEMENT DU PROJET PGI (21 points)

Question 1 : En fonction des tâches et contraintes d'antériorité (définies en annexe 2), proposer un graphe d'ordonnancement. Indiquer quel est le chemin critique et préciser la durée du projet (ne pas tenir compte des jours fériés).

Chemin critique : A - D - E - F - G - H - I - J - N - O - Q **Durée :** 181 jours.



Question 2 : Les développements complémentaires liés aux spécificités de l'activité s'avèrent plus complexes que prévu et vont finalement durer 40 jours. Quelles sont les conséquences de ce changement sur le graphe ? Justifier votre réponse.

Modification du chemin critique :

L'allongement de la durée des développements complémentaires fait que le chemin critique ne passe plus par la tâche J (paramétrages) mais par la tâche K (développements complémentaires).

Allongement de la durée du projet en raison de la modification du chemin critique :
La durée totale est allongée de 5 jours.

Question 3 : Proposer une solution pour compenser cet allongement et maintenir la durée initiale du projet. Justifiez votre proposition.

Il semble peu réaliste d'envisager de raccourcir la durée des contrôles. Donc il faut réduire l'une des deux tâches du chemin critique qui suivent immédiatement les développements : soit la réalisation de la documentation, soit la formation.

La documentation doit être terminée avant le début de la formation. Cela semble incontournable. Par contre elle inclut documentation technique et documentation utilisateurs. On peut envisager de dissocier ces deux aspects. La documentation technique pourrait être réalisée en parallèle de la réalisation des paramétrages et développements. De plus, cela semblerait plus logique d'en disposer pour la réalisation des tests. Conséquence : on gagne 5 jours car le chemin critique passe alors par les tests (15j) au lieu de la documentation (20j).

Concernant la formation, l'énoncé ne donne pas de précision sur les modalités d'organisation. On peut supposer que ce n'est pas tout le monde qui y participe pendant 20 jours, mais par groupes qui se succèdent. Il est sans doute possible, en ayant plus de formateurs, de mettre des groupes en parallèle, de façon que la durée totale soit ramenée à 15 jours, ce qui permettrait de rattraper les 5 jours de retard pris.

a supprimé: (Graphe : 7 points – Chemin critique : 3 points – Durée : 2 points soit 12 points)¶

a supprimé: (4 points)

a mis en forme : Police :5 pt

a mis en forme : Sans interligne, Espace Avant : 0 pt

a supprimé: (5 points)

a supprimé: CORRIGÉ ET BARÈME INDICATIF

DOSSIER 3 : SÉCURISATION DES ÉCHANGES (18 points)

Question 1 : Expliquer les conséquences des cyberattaques subies pour Mirlac. (Trois conséquences majeures sont attendues.)

L'intrusion d'un pirate dans le SI de Mirlac est dangereuse dans la mesure où celle-ci lui permettrait de récupérer ou supprimer des données confidentielles, d'y déposer des virus ou des logiciels malveillants dans le but de saboter le SI et le rendre inopérant.

La récupération de courriel est tout aussi dangereuse puisqu'elle signifie qu'un pirate peut intercepter le contenu de messages, à caractère confidentiel, circulant sur le réseau Internet entre deux personnes de la société. Pire, on pourrait imaginer que ce pirate usurpe l'identité de l'un deux et envoie des messages falsifiés ou erronés aux personnels de Mirlac dans le but de déstabiliser l'entreprise.

Une attaque par déni de service pourrait également être subie par Mirlac. Elle consiste à saturer un serveur ou un site Web d'entreprise afin de le rendre non opérationnel (empêcher les utilisateurs légitimes d'un service de l'utiliser ou de perturber les connexions entre les machines). Ce type d'attaque attaque peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès au serveur Web ou empêcher la distribution de courriels dans une entreprise. Dans le cas de Mirlac, ce type de cyberattaque peut paralyser son site Internet et empêcher ses partenaires d'accéder aux ressources mises en ligne par l'entreprise.

Question 2 : Après avoir défini ce qu'est un VPN, indiquer les clés de cryptage nécessaires en précisant de manière détaillée leur rôle lors d'un échange sécurisé par VPN depuis le siège à Angoulême vers l'usine de Challans.

Un VPN (Virtual Privatet Network) est un tunnel sécurisé établi entre deux sites lors d'un échange. Un VPN s'appuie sur le réseau Internet. Les informations sont cryptées à l'entrée et décryptées à la sortie. La sécurisation s'effectue par une clé de session (cryptage symétrique) préalablement envoyée par cryptage asymétrique.

Préalablement à tout transfert, chaque site génère son propre couple de clé publique/privée en vue d'un cryptage asymétrique et dépose sur un serveur de clés leur clé publique. On suppose que chaque site a donc récupéré la clé publique du site avec lequel il souhaite échanger de manière sécurisée.

L'envoi via un VPN suppose une clé de session.

1. L'émetteur (le siège) va générer un couple de clés identiques en vue d'un chiffrage symétrique.
2. Il va transmettre une de ces deux clés à sa division au moyen d'un cryptage asymétrique. Pour cela, le siège va crypter la clé de session avec la clé publique de l'usine de Challans et lui envoie.
4. À réception, l'usine de Challans utilisera sa clé privée (qu'elle seule possède) pour déchiffrer la clé de session reçue.
5. Les 2 sites possédant la même clé de session, l'échange crypté en asymétrique peut débuter.

Question 3 : Présenter quatre dispositifs, autres que le VPN, permettant à Mirlac de se prémunir des cyberattaques ou d'en limiter les conséquences. (3 X 1,5 point + 1 point = 5,5 points)

Pour se protéger contre les cyberattaques, Mirlac peut :

- renforcer le niveau de sécurité des machines connectées au réseau. Mettre dans une DMZ (DeMilitarised Zone), une zone tampon isolée du réseau privé de la société hébergeant des applications et des données mises à disposition du public, tous les serveurs contenant les applications importantes de Mirlac et son site Web;
- adopter une architecture composée de plusieurs serveurs offrant le même service, gérés de sorte que chaque client ne soit pris en charge que par l'un d'entre eux, ce qui permet de répartir les points d'accès aux services et en cas d'attaque d'avoir un ralentissement « acceptable »;

a supprimé: E
a supprimé: E
a supprimé: (3 X 1,5 point = 4,5 points)
a supprimé: (3 points + 5 points)
a supprimé: (3 points)
a supprimé: A
a mis en forme : Sans interligne, Espace Avant : 0 pt, Après : 0 pt
a supprimé: (5 points)
a supprimé: (1,5 point)
a supprimé: (1,5 point)
a supprimé: CORRIGÉ ET BARÈME INDICATIF

- mettre en place un serveur tampon (*cleaning center*) qui va filtrer et nettoyer le trafic et permettre que les requêtes malveillantes ne touchent pas le serveur visé ;
- identifier et bloquer les adresses IP dont proviennent les attaques au niveau du pare-feu ou du serveur. Cependant lorsque les attaques par déni de service sont distribuées cette méthode n'arrête pas l'attaque mais permet de la limiter.

Accepter toute idée pertinente.

Pour limiter les cyberattaques, Mirlac doit :

- mettre en place une politique de continuité d'activité destinée à élaborer des processus d'urgence et à définir les personnes à contacter en cas de perturbation, tout en sensibilisant les utilisateurs ;
- auditer de façon régulière le système d'information ;
- souscrire un contrat de cyber-assurance couvrant les risques informatiques évoqués.

Accepter toute idée pertinente.

a supprimé: (1 point)

a supprimé: (1,5 point)

a supprimé: (1,5 point)

a supprimé: (1 point)

a supprimé: (1 point)

a supprimé:
BARÈME¶
Questions
... [1]

a supprimé: CORRIGÉ ET BARÈME INDICATIF

Page 6 : [1] a supprimé fmarty 17/02/2019 15:38:00