SUJET GSE 2015
ÉLÉMENTS DE CORRIGÉ

PARTIE 1 : Gestion de l'information

A) Amélioration du processus de commandes par Internet

1.1	Identifier les dysfonctionnements actuels de la recherche de disponibilités via le formulaire du site internet de l'entreprise. **(annexes 1 et 2) (4 points)**

Les dysfonctionnements peuvent être multiples, on citera en particulier :

Dysfonctionnements	**Conséquences possibles (non attendues)**
Processus long et fastidieux	Risque d'abandon, de perte de temps de clients
Erreurs de saisie du client	Références incorrectes, renseignements erronés
Erreurs dans la recherche d'article par le commercial	Mauvaise information, mauvaise image de marque
Formulaire imprécis	

Argumentation possible :

Le processus est long car le client ne peut pas consulter le catalogue en ligne. Il est obligé de demander via le formulaire de commande, si l'entreprise propose le produit recherché.

Le commercial doit consulter la disponibilité des produits. Le client ne peut pas savoir en temps réel si les produits souhaités sont disponibles.

Il peut donc y avoir de nombreux échanges entre la recherche de référence et la recherche de disponibilité. Cela occasionne une perte de temps importante qui peut lasser le client.

Remarque : Accepter toute réponse pertinente.

C531.2 Représenter et analyser l'organisation du système d'information existant dans l'entreprise	4 points	**TS : 4 points** [identification d'au moins 3 dysfonctionnements] **S : 3 points** [identification de 2 dysfonctionnements] **I : 1 point** [identification d'un seul dysfonctionnement] **TI : 0 point** [réponse non adaptée]

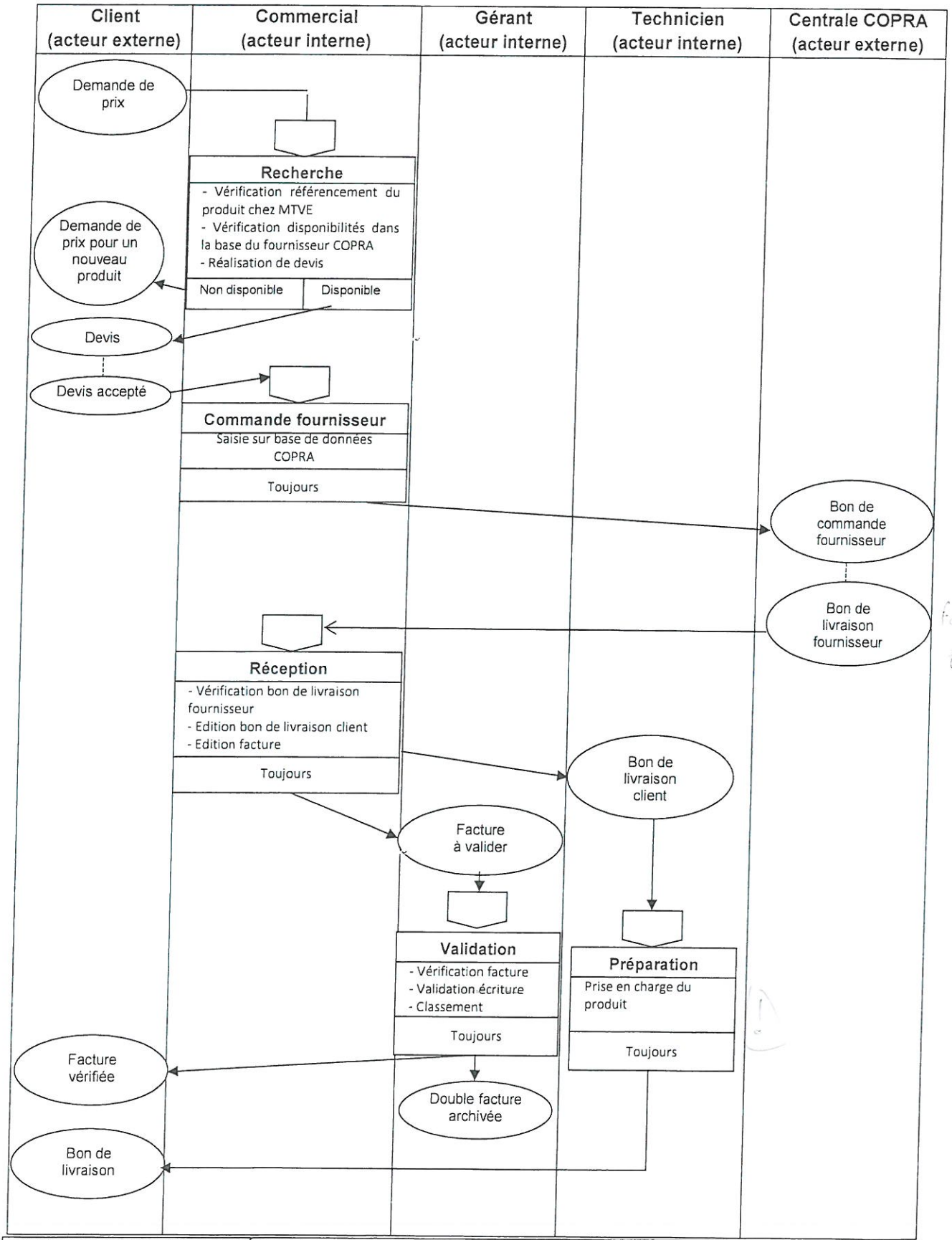
1.2	Compléter le diagramme évènement-résultat du processus de commande **(annexe A)** à partir du moment où le client accepte le devis d'après les informations fournies en **annexe 2. (8 points)**

Voir page suivante.

Remarque : on acceptera des éléments supplémentaires mais pertinents pour le processus, comme la prise de rendez-vous avec le client,

C531.2 Représenter et analyser l'organisation du système d'information existant dans l'entreprise	8 points	**TS : 8 points** [enrichissement du diagramme évènements-résultats : identification des activités, descriptions des activités avec les évènements déclencheurs, l'identification des tâches et les résultats corrects] **S : 7 – 4 points** [les activités sont partiellement présentées mais cohérentes avec le processus de même que pour les évènements et résultats] **I : 3 – 1 points** [le diagramme respecte les règles de formalisme du modèle] **TI : 0** [réponse non adaptée]

Annexe A : Schéma évènement-résultat du processus d'achat
Annexe à compléter et à rendre avec la copie



1.3	Déterminer les obligations du responsable du site en matière de droit à l'information dans le cadre de la collecte et du traitement des données nominatives. **(2 points)**

Pour l'évaluation on se réfère au barème. Les explications ci-dessous sont données à titre indicatif.

Les obligations des responsables de fichiers sont les suivantes :

Sécurité des fichiers

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende (art. 226-17 du code pénal).

La confidentialité des données

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc). La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende. La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende (art. 226-22 du code pénal).

L'information des personnes

Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits (d'accès, de rectification et d'opposition), les transmissions envisagées. Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 € par infraction constatée et 3 000 € en cas de récidive (art. 131-13 du code pénal).

L'autorisation de la CNIL

Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL. Le non-accomplissement des formalités auprès de la CNIL est sanctionné de 5 ans d'emprisonnement et 300 000€ d'amende (art. 226-16 du code pénal).

C532.1 Déterminer la nature et le volume des documents à conserver en respectant la réglementation	2 points	**TS : 2 points** [identification du caractère confidentiel des données personnelles enregistrées **ET** du besoin d'une déclaration à la CNIL **ET** mention sur droit d'accès, rectification, opposition] **S : 1,5 points** [identification du caractère confidentiel des données personnelles enregistrées **ET** besoin d'une déclaration à la CNIL **OU** mention sur droit d'accès, rectification, opposition] **I : 1 point** [déclaration à la CNIL **OU** identification du caractère confidentiel des données personnelles enregistrées **OU** mention sur droit d'accès, rectification, opposition] **TI : 0 point** [réponse non adaptée]	3/4 point abandon 2/4 1 1/4 0/4

B) Préparation de la négociation des achats d'électroménagers

1.4	Réaliser une requête permettant à M. Neveu d'avoir un état des produits (code du produit, désignation du produit, marque du produit et prix du produit) classés du plus cher au moins cher pour pouvoir négocier les prix. **(3 points)**

```
SELECT * ou idProduit, designation, marque, prixHT
FROM PRODUIT
ORDER BY prixHT DESC ;
```

C531.3 Interroger la base de données	3 points	**TS : 3 points** [identification des données nécessaires (on accepte une liste ou *), de la table, et de l'expression de tri] **S : 2 points** [absence de clause de tri **OU** présence de tables inutiles] **I : 1 point** [seulement identification des données] **TI : 0** [réponse non adaptée]

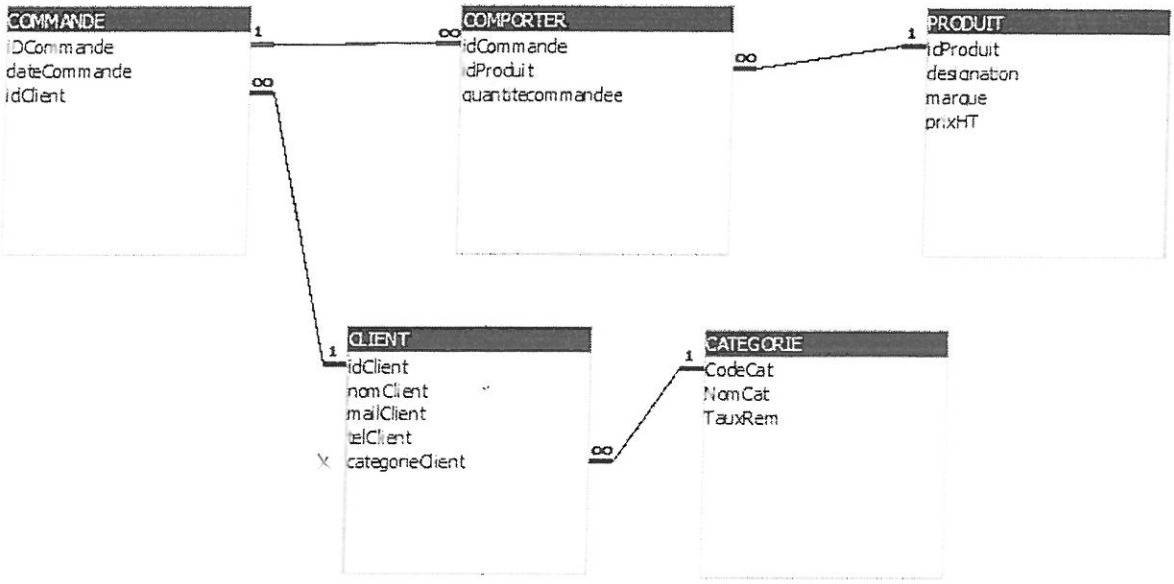
1.5	Réaliser la requête en langage SQL qui permet d'obtenir le montant des commandes (quantités commandées totales x prix de vente HT) réalisé par marque pour la période du 1er janvier 2014 au 31 décembre 2014. **(4 points)**

```
SELECT marque, SUM(quantitecommandee*prixHT) AS [CA annuel]
FROM COMPORTER,PRODUIT, COMMANDE
WHERE COMPORTER.idProduit=PRODUIT.idProduit
AND COMPORTER.idCommande=COMMANDE.idCommande
AND dateCommande BETWEEN #01/01/2014# AND #31/12/2014#
GROUP BY marque ;
```

Remarques : on ne se focalisera pas sur la syntaxe des formats de dates. On acceptera d'autres syntaxes pour les critères de dates (dateCommande LIke « *2014 » ou dateCommande >= '01/01/2014' AND dateCommande <= '31/12/2014'

C531.3 Interroger la base de données	4 points	**TS : 4 points** [identification des données nécessaires (on accepte une liste ou *), des tables, des jointures, de la restriction et de l'expression de tri **S : 3 – 2 points** [absence de jointure **ou/et** fonction SUM mal définie **ou/et** absence de regroupement ou/et absence de restriction] **I : 1 point** [seulement identification des données] **TI : 0** [réponse non adaptée]

1.6	Indiquer sur votre copie les modifications à réaliser sur le schéma relationnel pour prendre en compte cette demande (ne faire apparaitre que les relations modifiées ou ajoutées). **(3 points)**



On vérifie la présence d'une clé étrangère dans la table CLIENT. Le fait de la renommer n'est pas obligatoire.

On ne sanctionne pas une erreur sur le formalisme ∞ ou 1

On acceptera la création d'une table supplémentaire REMISE liée à la table CATEGORIE

C531.5 Proposer des améliorations et des ajustements	3 points	**TS : 3 points** [création d'une nouvelle table categorie, création de trois propriétés adaptées dans la table categorie et relation cohérente entre les deux tables] **S : 2 points** [création d'une nouvelle table, champs manquants **OU** pas de lien entre categorie et client] **I : 1 point** [ajout de la remise dans la table client] **TI : 0** [réponse non adaptée]

Partie 2 : Participation à la gestion des risques informatiques

2.1	Proposer un paramétrage complet à mettre en place sur le poste de travail permettant aux deux nouvelles stations de se connecter au réseau local et au réseau internet **(annexe 5 et annexe 6). (3 points)**

Il convient de choisir deux adresses IP non utilisées.

Par exemple :

Nouveau poste 1 : 192.168.2.24

Nouveau poste 2 : 192.168.2.25

On doit également indiquer l'adresse du routeur soit 192.168.2.149 (passerelle par défaut) pour obtenir un accès à Internet et le masque de sous-réseau (255.255.255.0).

2.2	Présenter une solution permettant d'obtenir une adresse IP automatiquement lors de la connexion d'un nouveau matériel sur le réseau. **(2 points)**

Le DHCP (acronyme de Dynamic Host Configuration Protocol) permet de distribuer des adresses IP sur les hôtes d'un réseau. Chaque station ou imprimante nouvellement installée se verra attribuée une adresse IP de façon automatique en fonction des plages d'adresses disponibles et de celles qui sont déjà utilisées.
L'utilisation de ce protocole nécessite l'installation du service DHCP (ou serveur DHCP) sur un serveur de l'entreprise.
Cette solution permettra à l'entreprise Neveu d'éviter la recherche d'une adresse disponible (Cf 2.1) si le parc informatique connecté au réseau se développe.
La référence à l'usage du WiFi ne répond pas à la demande car ne concerne que la connexion physique au réseau (par une liaison sans fil).

C711.2 Définir et mettre en œuvre la politique de sécurité avec l'interlocuteur informatique	2 points	**TS : 2 points** [DHCP proposé avec référence à l'installation d'un serveur/service DHCP] **S : 1 point** [DHCP proposé] **TI : 0** [réponse non adaptée]

2.3	Suggérer une solution à M. Neveu pour prévenir et traiter chaque problème rencontré. Vous présenterez votre travail sous la forme d'un tableau. **(6 points)**

(voir page suivante)

C711.3 Contrôler la mise en œuvre par les utilisateurs des procédures de sécurité	6 points	**TS : 6 points** [Propositions cohérentes et complètes- les solutions proposées évoquent trois types de risques : les risques humains, matériels et logiciels] **S : 5 – 4 points** [Propositions cohérentes mais incomplètes, deux catégories de risques apparaissent] **I : 3 – 1 point** [Propositions incomplètes, seule une catégorie est proposée] **TI : 0** [réponse non adaptée] Bonus + 1

Bonus de un point pour le candidat qui distingue prévention et traitement.

La présentation du tableau peut être différente de celle proposée ci-dessous.

N°	Date	Problème constaté	Solutions proposées
1	24/07/2012	Problème de mise à jour automatique de l'antivirus. La mise à jour s'établit manuellement toutes les deux semaines depuis ce jour.	- Acquérir un logiciel antivirus/antispam efficace permettant une mise à jour automatique. - Vérifier la mise à jour du logiciel et la mise à jour des bases virales. - Faire des scans à la recherche des virus et des malwares. - Faire des mises à jour régulières des applications.
2	03/08/2012	Température de 38°C relevée dans le local réseau, arrêt temporaire du serveur. Redémarrage le 06/08/2012.	Acquérir un système de climatisation permettant de réguler la température et de préserver le matériel puis solutions de sauvegardes régulières à mettre en œuvre en cas de problème.
3	18/03/2013	Deux collaborateurs utilisent le même mot de passe, suite à la perte d'un mot de passe réseau par l'un d'entre eux (les mots de passe qu'ils ont créés librement contiennent 4 caractères).	- Adoption d'une charte de sécurité pour interdire l'échange des mots de passe. - Les identifiants et les mots de passe doivent être sécurisés. Utilisation de sites permettant de tester les mots de passe le cas échéant. - Le mot de passe doit associer des lettres majuscules et minuscules, ainsi que des chiffres, le nombre de caractères doit être augmenté au-delà de 4 caractères. - Les mots de passe doivent être changés régulièrement. - On peur également envisager une formation ou information générales des collaborateurs face aux risques
4	25/07/2013	Suite à un violent orage, une carte réseau défectueuse et une alimentation d'un poste ont été changés.	- Acquisition d'un onduleur qui permet de faire face aux problèmes de surtension ou de coupure de courant - Sauvegardes régulières des données
5	24/03/2014	Un disque du serveur hors service, saisie des journées du 20/03/2014 et 21/03/2014 à reprendre, une copie de sauvegarde avait été réalisée le 19/03/2014.	- La sauvegarde incrémentielle journalière dysfonctionne donc parfois : s'interroger sur le support utilisé, peut être est-il plein en écriture. Dans ce cas, il faut changer les supports régulièrement. - Mettre en place la sauvegarde complète (et éventuellement différentielle) et dans ce cas former l'assistante à cette sauvegarde. - La solution repose avant tout sur la politique de sauvegarde à mettre en œuvre : fréquence, durée de conservation des supports, fréquence de réutilisation, planification.

6	02/04/2014	Mail reçu de notre banque visant à fournir nos références bancaires pour vérification. La banque a été contactée mais n'est pas à l'origine de cette demande.	- Il ne faut pas fournir les données demandées car il s'agit d'une tentative de piratage. - Prévenir les organismes concernés (banque…) des tentatives de phishing. - Filtre antiphishing. - Formation/information

2.4	Dans une note structurée, vous présenterez les risques liés à la pratique du BYOD ainsi que les solutions à mettre en place pour limiter ces risques. **(5 points)**

Emetteur : L'assistant(e) de gestion
Destinataire : Monsieur Neveu, Directeur

Date : date de l'examen

NOTE DE TRAVAIL

Objet : les risques liés à la pratique du BYOD

Source :
ANSSI

La pratique du BYOD se développe et conduit à nous interroger sur les risques potentiels pour l'entreprise et les solutions qui peuvent être envisagées pour les limiter.

I. Les risques potentiels de la pratique du BYOD

Les risques peuvent être les suivants :

- vol ou perte du terminal ;
- exploitation d'une faille du système d'exploitation (IOS, Android...) notamment sur les terminaux non protégés (« *jailbreakés* » ou « *rootés* ») ;
- exploitation d'une faille d'une application ;
- installation d'une application comprenant un cheval de Troie qui permettra de diffuser les données contenues dans le terminal ;
- accès au terminal via une connexion WiFi ou Bluetooth non sécurisée ;
- exploitation d'une faille du navigateur (ou d'une application java) du terminal.

II. Les solutions à envisager pour limiter ces risques

Les solutions qui peuvent être mises en œuvre sont les suivantes :

- configurer une durée d'expiration du mot de passe ;
- configurer le verrouillage automatique de terminal au bout de 5 minutes maximum ;
- limiter le nombre de tentatives de déverrouillage, puis configurer un temps de blocage de plus en plus long ainsi qu'un effacement automatique après une dizaine de tentatives ayant échoué ;
- ne pas laisser le terminal sans surveillance. Un accès très temporaire à un terminal mobile peut suffire à sa compromission sans que l'utilisateur en ait conscience même lorsqu'il est verrouillé ;
- ne pas brancher le terminal à un poste de travail non maîtrisé ou à un quelconque périphérique qui ne soit pas de confiance ;
- interdire l'installation d'applications non explicitement autorisées par l'entreprise. Cette recommandation vaut également pour les applications préinstallées ;
- les applications déployées doivent être mises à jour régulièrement et rapidement dès lors que des correctifs de sécurité sont proposés ;
- les interfaces sans-fil (Bluetooth et WiFi) ou sans contact (NFC par exemple) doivent être désactivées lorsqu'elles ne sont pas utilisées ;

- désactiver systématiquement l'association automatique aux points d'accès WiFi configurés dans le terminal afin de garder le contrôle sur l'activation de la connexion sans-fil ;
- le stockage amovible ainsi que le stockage interne du terminal doivent être chiffrés par l'utilisation d'une solution de chiffrement robuste ;
- tout échange d'informations sensibles doit se faire par un canal chiffré de manière à assurer confidentialité et intégrité des données (utilisation d'un VPN) ;
- le système d'exploitation doit être régulièrement et automatiquement mis à jour de manière à intégrer les derniers correctifs de sécurité publiés. Tout terminal qui ne peut plus prendre en charge les évolutions du système d'exploitation doit être remplacé ou ne plus être autorisé pour un usage professionnel.

Il convient donc de sensibiliser les salariés aux risques liés aux usages des terminaux mobiles et de mettre en place les solutions envisagées.

Accepter les risques comportementaux.
Accepter également la mise à disposition d'équipements (tablettes, smartphones...) par l'entreprise.

L'assistant de gestion

C711.1 Définir et mettre en œuvre la politique de sécurité informatique	5 points	**TS : 5 points** [Le plan est structuré, on trouve au moins 3 risques et 3 solutions. La note n'est pas forcément introduite et la conclusion n'est pas exigée] **S : 4-3 points** [Le plan est structuré, on trouve au moins 2 risques et 2 solutions. La note n'est pas forcément introduite et la conclusion n'est pas exigée.] **I : 2-1 point** [La note n'est pas forcément structuré, on trouve au moins 1 risque et 1 solution.] **TI : 0** [réponse non adaptée]