BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2022

RECOMMANDATIONS POUR L'ÉLABORATION D'UN SUJET POUR L'ÉPREUVE E6 « CYBERSÉCURITÉ DES SERVICES INFORMATIQUES »

La construction d'un sujet de niveau BTS est une mission de confiance qui sollicite une part importante des compétences professionnelles de la professeure ou du professeur. C'est un rendez-vous privilégié avec sa propre lecture du référentiel du diplôme et souvent une occasion de revisiter son enseignement.

Compte tenu de la diversité des compétences évaluées dans cette épreuve, les auteurs sont réunis en équipe, autour d'une ou d'un chef de projet désigné(e) par l'équipe. Leurs rôles sont précisés dans ce document.

L'ensemble de l'équipe est responsable de la contribution demandée et doit veiller collectivement au respect scrupuleux des délais et de la confidentialité de ses travaux.

La conformité de la proposition de sujet au référentiel du diplôme[1] et à la définition de l'épreuve (arrêté du 29 avril 2019) est la première condition de sa recevabilité.

Les noms et le contenu des fichiers constituant le sujet, le corrigé et le barème ne doivent comporter aucune information permettant d'en identifier la nature : pas de référence au nom de l'examen ni au millésime de la session notamment. Ces indications, comme la première page du sujet, seront ajoutées par la suite.

[1] Le référentiel est disponible à la page https://enqdip.sup.adc.education.fr/bts/index.htm

Contenu

Rappel de la définition des épreuves

Épreuve E6 - Option « Solutions d'infrastructure, systèmes et réseaux »

Cybersécurité des services informatiques

Épreuve écrite – Coefficient 4

1 – Objectif

Cette épreuve vise à évaluer chez la personne candidate l'acquisition des compétences décrites dans le bloc de compétences « Cybersécurité des services informatiques » pour l'option « Solutions d'infrastructure, systèmes et réseaux», à savoir :

- protéger les données à caractère personnel ;
- préserver l'identité numérique de l'organisation ;
- sécuriser les équipements et les usages des utilisateurs ;
- garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ;
- assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service.

2 - Critères d'évaluation

Les critères d'évaluation correspondent aux critères de performance exprimés pour chaque compétence du bloc « Cybersécurité des services informatiques » pour l'option « Solutions d'infrastructure, systèmes et réseaux » figurant dans le référentiel de compétences (annexe I.B).

3 – Modalités d'évaluation : épreuve ponctuelle écrite, durée 4 heures

Cette épreuve est écrite, elle se déroule sous forme ponctuelle.

L'épreuve revêt la forme d'une étude de cas de production de services informatiques sécurisés, construite à partir d'une situation réelle, mobilisant les ressources décrites pour le bloc « Cybersécurité des services informatiques ». Elle est composée de plusieurs dossiers couvrant différentes missions dans le domaine des solutions d'infrastructure, systèmes et réseaux. Elle comporte un dossier documentaire permettant de situer le contexte de l'organisation, les solutions applicatives et d'infrastructure mises en œuvre, les moyens techniques, humains, financiers disponibles, le cadre juridique, l'expression des besoins ayant motivé les services demandés.
La correction est assurée par une personne enseignante en charge d'un bloc professionnel en section de techniciens supérieurs « Services informatiques aux organisations ».

Épreuve E6 - Option « Solutions logicielles et applications métiers »

Cybersécurité des services informatiques

Épreuve écrite – Coefficient 4

1 – Objectif

Cette épreuve vise à évaluer chez la personne candidate l'acquisition des compétences décrites dans le bloc de compétences « Cybersécurité des services informatiques » pour l'option « Solutions logicielles et applications métiers », à savoir :

- protéger les données à caractère personnel ;
- préserver l'identité numérique de l'organisation ;
- sécuriser les équipements et les usages des utilisateurs ;
- garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ;
- assurer la cybersécurité d'une solution applicative et de son développement.

2 - Critères d'évaluation

Les critères d'évaluation correspondent aux critères de performance exprimés pour chaque compétence du bloc « Cybersécurité des services informatiques » pour l'option « Solutions logicielles et applications métiers » figurant dans le référentiel de compétences (annexe I.B).

3 – Modalités d'évaluation : épreuve ponctuelle écrite, durée 4 heures

Cette épreuve est écrite, elle se déroule sous forme ponctuelle.

L'épreuve revêt la forme d'une étude de cas de production de services informatiques sécurisés, construite à partir d'une situation réelle, mobilisant les ressources décrites pour le bloc « Cybersécurité des services informatiques ». Elle est composée de plusieurs dossiers couvrant différentes missions dans le domaine des solutions logicielles et applications métiers. Elle comporte un dossier documentaire permettant de situer le contexte de l'organisation, les solutions applicatives et d'infrastructure mises en œuvre, les moyens techniques, humains, financiers disponibles, le cadre juridique, l'expression des besoins ayant motivé les services demandés.

La correction est assurée par une personne enseignante en charge d'un bloc professionnel en section de techniciens supérieurs « Services informatiques aux organisations ».

L’équipe de concepteurs

Rôle de l’équipe

L’équipe, qui rassemble des compétences permettant de concevoir un sujet complet (dans les domaines technologique, économique, juridique et managérial) est chargée de :

- choisir le contexte organisationnel qui servira de point d’appui à l’ensemble du sujet et de définir le scénario d’évaluation (problématique d’ensemble et thèmes des parties) ;
- participer aux réunions organisées en ligne avec les réviseurs afin de définir en commun la trame du sujet et apporter les informations complémentaires utiles à son propos ;
- s’assurer que les noms de organisations et les documents peuvent être utilisés, donc
    - vérifier que les données réelles peuvent être légitimement utilisées pour la conception d’un sujet : autorisation formelle obtenue auprès des organisations (modèle en **annexe 5**) ou données publiques (explorer le site internet[2]) ;
    - vérifier les droits des images utilisées dans le sujet ;
    - démarquer si besoin : « Démarquer » signifie proposer un autre nom pour l’organisation ou pour un outil, après avoir vérifié que ce nom ne renvoie à rien de semblable.

Rôle de la ou du chef de projet

L’équipe désigne une ou un chef de projet en charge de :

- organiser au mieux la répartition des responsabilités au sein de l’équipe et de fixer ses modalités de fonctionnement ;
- coordonner les phases de conception, rédaction et validation de la proposition ;
- au besoin, représenter l’équipe durant les réunions si la, le ou les autres membres ne peuvent être disponibles ;
- suivre la mise au point du sujet, en relation avec chaque membre de l’équipe ;
- transmettre la proposition de sujet et son corrigé contenant tous les documents nécessaires à la reconstitution électronique complète du sujet en précisant les noms des logiciels utilisés pour élaborer les schémas, les illustrations ou copies d’écran.

[2] L’utilisation de l‘extrait d’un site *Web* suppose l’obtention d’une autorisation suivant les mentions légales indiquées.

Choix du contexte organisationnel

Le choix et la rédaction du contexte organisationnel constituent une première étape essentielle du travail de l'équipe avant d'engager la rédaction des différentes missions qui seront confiées aux candidats.

Il est nécessaire de situer la candidate ou le candidat dans une posture conforme aux indications du référentiel de compétences[3], à savoir :

«*La personne titulaire du diplôme exerce des activités pour répondre aux besoins de sécurité des services informatiques d'une organisation cliente notamment au regard du développement des menaces et attaques en provenance du cybermonde et des risques liés aux usages numériques. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.* »

Ainsi le sujet doit clairement mettre en évidence :

- une organisation cliente (son métier, ses processus, ses acteurs et son système d'information) qui commande un service informatique ;
- une organisation prestataire de services informatiques (description du prestataire informatique et des modalités de gestion du système d'information), interne à l'organisation cliente (DSI) ou externe (ESN), pour laquelle la candidate ou le candidat intervient ;
- la relation de service entre ces deux organisations (contrat de prestation de service) ;
- en tant que de besoin, la description du système informatique, les référentiels, normes et méthodes adoptés au sein de l'organisation, l'environnement matériel et logiciel, etc.

Il est impératif de prendre appui sur la situation d'une organisation réelle pour la réalisation du sujet. L'activité des organisations choisies ne doit pas porter à polémique en lien avec l'actualité ou encore des considérations éthiques, politiques ou religieuses.

La conduite d'entretiens et la collecte de documents auprès de cette organisation seront de précieuses sources d'informations pour documenter le sujet et nourrir son questionnement. **L'annexe 1** du présent document propose des pistes pour le recueil d'informations au sein d'une organisation en vue de la préparation d'un sujet.

Définition du scénario support du sujet

Le scénario constitue le fil conducteur du sujet ; il donne sens aux réalisations demandées par rapport aux besoins et aux contraintes des organisations présentées. Il est orienté « métier » (réseau/système/service en SISR et données/traitements en SLAM) puisque l'épreuve est propre à l'option.

Ce fil conducteur doit être explicité en fin de présentation du contexte.

[3] Un extrait du référentiel de compétences concernant le bloc « Cybersécurité des services informatiques » est présenté en annexe 2.

La candidate ou le candidat doit pouvoir comprendre rapidement dans quel but et dans quel cadre les travaux sont demandés.

Dans ce scénario, la candidate ou le candidat est placé en situation de jouer un rôle actif au sein de l'organisation prestataire pour répondre à une ou plusieurs demandes de service de l'organisation cliente. Son action doit s'appuyer sur des ressources (cahier des charges, ticket d'incident, etc.) qu'elle ou il est invité à analyser avant de prendre en charge tout ou partie des missions qui lui sont confiées.

Durant la phase d'élaboration du scénario, il est recommandé de réaliser une sélection précise des compétences dont l'évaluation est recherchée dans le sujet. Ceci doit permettre de s'assurer qu'un éventail assez large de compétences est évalué. Ce sont uniquement les compétences du bloc "Cybersécurité des services informatiques" (bloc 3) qui sont évaluées dans l'épreuve.

La partie du référentiel de compétences associée au bloc 3, reprise en **annexe 2**, constitue donc la référence pour définir la substance du sujet et le questionnement : la rubrique « indicateurs de performance » associée à chaque compétence permet d'orienter l'évaluation, la liste des savoirs associés aide à la formalisation des questions. À ce sujet, il est rappelé que les savoirs sont de deux natures : des savoirs technologiques et des savoirs économiques, juridiques et managériaux.

Dès cette phase de conception, **la contrainte de la durée de l'épreuve (4 heures),** incluant temps de lecture du sujet et de rédaction de la copie, devra être intégrée. De même, il est essentiel de situer la difficulté du sujet à un niveau compatible avec les exigences habituelles des enseignants ou formateurs.

Contexte et scenario donneront lieu à validation lors d'une webréunion fin juin 2020.

Élaboration du sujet

Le sujet débute par une présentation des principaux éléments de contexte. Il est ensuite structuré en dossiers. Une documentation est fournie en annexe du sujet.

Construction du sujet en dossiers et missions

Un dossier définit une finalité générale d'intervention pour la technicienne ou le technicien dans un contexte en rapport avec un enjeu de cybersécurité pour une organisation donnée. Celle-ci donne du sens à l'ensemble des missions, même si celles-ci sont effectuées dans des contextes spécifiques (acteurs, lieux, temps, ressources, etc.).

Chaque dossier est indépendant et permet d'évaluer une ou plusieurs compétences du bloc 3 (pages 43 à 48 du référentiel, reprises en **annexe 2**).

Une mission correspond à un objectif clairement défini dans un contexte spécifique pour lequel des actions mobilisant des compétences du bloc 3 doivent être réalisées. Une mission engage la responsabilité de celle ou celui qui l'ordonne et de celle ou celui qui l'effectue.

Le questionnement invite les candidats à réaliser des tâches qui nécessitent de s'appuyer sur une documentation. Les éléments techniques associés doivent se trouver dans le dossier documentaire plutôt que dans le corps du sujet.

Rédaction du sujet

Le vocabulaire spécifique au domaine traité dans le sujet (« vocabulaire métier »), s'il n'appartient pas au domaine de l'informatique ou s'il est trop dépendant des outils utilisés, doit être systématiquement explicité : dans le corps du texte, en note de bas de page ou à l'aide d'un lexique inséré dans le dossier documentaire.

Il convient d'être particulièrement attentif à la cohérence du langage et des notations informatiques utilisés, à la qualité rédactionnelle des textes du sujet et du corrigé, à la rigueur de la ponctuation et au respect des usages en matière d'écriture et de disposition de textes et tableaux. **L'annexe 3 présente les recommandations d'usage de la langue française.**

Les concepts et les méthodes des référentiels de bonnes pratiques doivent être utilisés mais sans considérer que les candidats connaissent en détail le contenu de ces référentiels. Ainsi, autant que nécessaire, les termes et principes tirés de ces référentiels seront explicités dans le sujet.

Les formulations et les questionnements qui permettent **d'éviter l'usage de la calculatrice** (calculs simples ou résultats numériques donnés) seront privilégiés.

Il est recommandé d'éviter tout document-réponse (annexe) à compléter et à rendre avec la copie.

Nommage des différentes parties du sujet

Outre les consignes fournies dans le modèle de document pour la rédaction du sujet, il convient d'adopter les règles suivantes :

- Le sujet porte habituellement le nom de l'organisation cliente étudiée dans le cas.
- Il est organisé en dossiers. Les dossiers sont identifiés par une lettre et portent un intitulé significatif du service rendu à l'organisation cliente sous forme d'activité : par exemple, « Dossier A – Participation à l'atelier d'analyse des risques liés à l'application *Web* » ou « Dossier B – Audit et évolution de l'infrastructure réseau ».
- Les missions sont numérotées de 1 à n dans chaque dossier.
- Le numéro d'une question est préfixé avec le numéro de la mission et la lettre du dossier : exemple, B.4.2. pour la deuxième question de la quatrième mission du dossier B.
- Les missions portent un nom significatif de l'objectif confié à la candidate ou au candidat : par exemple, « Mission 3 – Prise en compte du règlement général sur la protection des données (RGPD) dans les récits utilisateurs » ou « Mission 2 – Paramétrage du dispositif de sécurité ».
- **L'annexe 4** liste les conventions concernant les modèles et les schémas.

Rédaction des questions dans le sujet

La rédaction des questions doit faire l'objet d'un soin particulier car elle conditionne directement la juste interprétation par la candidate ou le candidat du travail à faire.

On veillera notamment à respecter les règles suivantes :

- Les questions sont courtes, claires, aisément compréhensibles ; elles n'excèdent pas une phrase et se rapporte directement au texte du sujet qui précède la question.
- Les questions commencent par un verbe à l'infinitif[4] : « expliquer », « présenter », «calculer », etc.
- Les questions doivent exclure l'apport d'informations préalables ou complémentaires ; celles-ci sont mentionnées dans texte du sujet ou dans le dossier documentaire.
- Les questions font sens dans le contexte du sujet, elles doivent permettre de répondre à un besoin de l'organisation cliente exprimé dans le sujet ; il n'y a pas de question de cours qui solliciterait la seule restitution d'un savoir.
- Les questions ne sont pas entièrement dépendantes de la justesse d'une réponse donnée à une question précédente. Si la réponse d'une question nécessite d'avoir répondu correctement à une question précédente, les questions dépendantes sont rassemblées en une seule phrase comportant plusieurs consignes notées a) b) c), etc.
- Les réponses attendues doivent pouvoir être évaluables de manière fiable et objective, elles doivent correspondre aux attentes d'une épreuve écrite. Il est exclu de questionner sur des éléments qui sont liés aux fonctionnalités d'un logiciel ou d'un équipement spécifique que les candidats pourraient ne pas connaître.

Nature du questionnement

Un questionnement sur le cœur de métier de chaque option

Le sujet évalue les compétences communes aux deux options et celles spécifiques à l'option. Concernant les compétences communes, elles sont évaluées en fonction du métier visé par l'option du diplôme. En effet, les tâches à accomplir ne seront pas les mêmes pour un technicien réseau et un technicien développeur. Ceci implique de considérer l'évaluation de chaque compétence, y compris celles qui sont communes, en fonction de l'option.

Exemple : si on veut évaluer la compétence commune suivante « *Recenser les traitements sur les données à caractère personnel au sein de l'organisation »*
Le guide d'accompagnement du référentiel[5] explique :
"Cette compétence implique d'identifier les données à caractère personnel, les traitements sur ces données mais aussi les supports et les équipements sur lesquels sont stockées ou traitées ces données. Cela a le mérite de donner très rapidement la mesure des tâches à accomplir pour respecter la réglementation."
Ainsi, pour l'option SISR, pour évaluer cette compétence, on s'intéressera plutôt ici (par exemple) à la sécurité du stockage et de l'accès au stockage en ligne ou localement.
Pour l'option SLAM on s'intéressera plutôt ici (par exemple) au respect, par les traitements, de la réglementation sur ces données (consultation, copie, effacement, anonymisation, etc.), aux structures de données (normalisation), à la sécurité des API d'accès (authentification) et aux données circulant sur le réseau via les formats d'échanges ouverts (Json, XML , etc.) .

[4] Les auteurs pourront exploiter la taxonomie de Bloom qui vise à aider les enseignants dans la rédaction de consignes : http://fr.wikipedia.org/wiki/Taxonomie_de_Bloom
[5] Le guide est disponible à la page https://www.reseaucerta.org/sio2019/accueil

Une prise en compte des dimensions économique, juridique et managériale des compétences du référentiel

Les compétences décrites dans le référentiel de compétences pour le bloc « Cybersécurité des services informatiques » mobilisent des savoirs économiques, juridiques et managériaux (cf. **annexe 2**). Les questions qui sollicitent ces savoirs doivent faire sens dans le questionnement, le contexte et la problématique proposés dans le sujet.
Les responsabilités métiers (technicien réseau, développeur) offrent une piste de questionnement intéressante.

Exemples :
Option SISR
« On constate qu'une habilitation donne le droit à l'administrateur d'accéder aux courriels des utilisateurs :

- expliquer pourquoi cette habilitation ne respecte pas la réglementation ;
- proposer une modification. ».

Option SLAM
« On constate que les connexions (*log*) programmées contiennent des données à caractère personnel non anonymées :

- rédiger un courriel à l'attention des programmeurs leur expliquant pourquoi les connexions (*log*) doivent être modifiées ;
- proposer aux programmeurs une modification de leur programme. ».

Une articulation sûreté / sécurité ou qualité / sécurité permettant un questionnement métier intégré dans une orientation cybersécurité

Assurer la sécurité nécessite de s'appuyer sur une base sûre. Donc le questionnement pourra porter aussi bien sur la vérification de la sûreté que sur la mise en place de la sécurité face à des interventions malveillantes.
Par exemple, si dans un sujet de l'option SISR la tolérance n'est pas assurée correctement pour un stockage serveur, on peut demander aux candidats de proposer une solution après avoir exposé sa critique de l'existant.
Dans un sujet de l'option SLAM, il ne s'agit pas par exemple de demander la conception complète d'un schéma de données. Mais, afin de répondre à un besoin de sécurité, il est possible de demander la vérification d'un schéma de données et, si le cas échéant la prise en charge des évolutions nécessaires pour garantir la sécurité ou le respect de la réglementation. Dans le cadre de la sécurité, il sera possible de montrer du code redondant (qui implique une mise en facteur) et demander sa réécriture. De même, il est possible de montrer des tests défectueux ou encore de demander une correction du code si ces évolutions sont associées à des préoccupations de cybersécurité.

Voici d'autres exemples.
Option SISR :
« On observe qu'un utilisateur dispose d'une liste de contrôle d'accès (*Access Control List –ACL-*) directement sur des ressources et non à travers des groupes d'utilisateurs :

- expliquer en quoi ces habilitations posent un problème de sécurité ;
- proposer une modification. »

Option SLAM
« Une règle de gestion limite la valeur maximum d'une propriété à 12. On observe que le contrôle est fait dans le programme utilisant la classe et non dans la classe :
- expliquer en quoi la programmation de la classe pose un problème de sécurité ;
- proposer une modification (*on attend une modification du mutateur de la propriété).* »

Pour l'option SISR, un questionnement sécurité enrichi

La sécurité pour l'option SISR était déjà présente dans l'ancienne épreuve E5, de nombreux sujets abordent d'ailleurs cette préoccupation. Elle constitue désormais une épreuve à part entière et son questionnement est de ce fait enrichi.
Des pistes nouvelles de questionnement peuvent être explorées, notamment sur l'intégration de la sécurité dans une démarche projet, sur le respect de la réglementation (en référence au RGPD), sur les contrats de prestation de services, sur les tableaux de bord de sécurité informatique, sur la qualification des matériels d'interconnexion, sur les accès nomades, sur le risque potentiel des mesures telles que AVEC (*BYOD*), etc. Bref, la liste des questions possibles est longue.
Aujourd'hui toutes les organisations ont mis en place des dispositifs de sécurité et malgré cela, nombreuses ont été victimes d'attaques.
Par exemple, à l'heure où sont écrites ces lignes, la société Bouygues et la région Grand Est ont été victimes d'une attaque informatique qui a bloqué leur système. Dans le second cas des données sensibles auraient fuitées.
Des scénarios sont souhaitables autour de la prévention, détection et réparation, etc.
La difficulté sera sans doute d'avoir accès à des informations souvent confidentielles et de veiller à ne pas les divulguer.

Pour l'option SLAM, un questionnement sécurité novateur qui reste axé sur le métier

La préoccupation de cybersécurité est relativement nouvelle dans l'examen, voici quelques pistes permettant de la prendre en charge.
Sur le fond, le questionnement porte sur les objets métier liés au développement autour des données et des traitements ; il s'agit de produire des éléments de schémas de données, de requêtes, du code objet, etc.
On doit aussi intégrer au questionnement les outils de sécurité associés aux méthodes d'analyse, à l'environnement de développement et au respect de la réglementation (RGPD notamment).
On peut s'intéresser aux différentes étapes d'un développement (sans préjuger de la méthode respectée), aux objets et aux outils associés pour explorer des pistes de questionnement.
Il s'agit naturellement de rester focalisé sur le cœur de métier de l'option SLAM. On introduit cependant fortement la question du risque dès la conception d'une application (atelier d'analyse du risque, événements redoutés, etc.).

Voici une proposition de thèmes potentiels pouvant inspirer les dossiers du sujet :
- atelier d'analyse du risque : récits utilisateurs, scénarios de risques (*abusers stories*), évènements redoutés, etc. ;

- validité et sécurité des données : critique existant, construction de ce qui est nécessaire pour respecter le RGPD, anonymisation, limitation des données personnelles, etc. ;
- accès aux données : requêtes, sécurité des comptes, optimisation requêtes, renvoi de données personnelles non nécessaires ou erronées, requêtes pour tester des anomalies, requêtes sur fichier de connexions, etc. ;
- programmation dont programmation orientée objet (POO) : prise en compte des traitements pour le respect du RGPD, problématiques associées à l'authentification, exploitations des connexions (*logs*), interface. de programmation (*API*) d'accès, gestion des sessions, responsabilité des classes, sécurité des vues, etc.) ;
- gestion de l'environnement de développement et de tests : protection poste de travail du développeur, composants certifiés, jeu d'essai, gestion de versions, etc..

Composition de la documentation fournie en annexe du sujet

Les documents annexés au sujet ont principalement pour but de permettre à la candidate ou au candidat d'appréhender le plus précisément et le plus rapidement possible le contexte dans lequel il lui est demandé d'intervenir. Il s'agit aussi de placer la réflexion de la candidate ou du candidat sur un autre terrain que celui de la mémorisation de techniques, protocoles ou normes. Cette documentation peut comporter un lexique ainsi que des explications concernant des normes, technologies ou outils dont les auteurs estiment qu'ils ne sont pas toujours nécessairement connus de l'ensemble des candidats. **On veillera à ce que les outils à mobiliser pour traiter le sujet ne pénalisent pas ou ne favorisent pas certains candidats.**

Concernant la documentation, le respect des conseils suivants est impératif :

- limiter strictement le nombre et la densité des documents de façon à ne pas nécessiter un temps de lecture excessif par rapport à la durée de l'épreuve. On estime qu'un **temps de lecture d'une heure** est un maximum ;
- fournir des extraits significatifs et adaptés de préférence à la version intégrale ;
- fournir impérativement dans l'archive livrée, les fichiers source des documents insérés dans le sujet ;
- indiquer impérativement la source des documents si les auteurs du sujet n'en sont pas à l'origine (publication, date, nom de l'auteur, page, etc.), préciser s'il s'agit d'un extrait (« extrait de… » ou « adapté de… ») et s'assurer de l'autorisation d'utilisation ;
- en cas d'utilisation de documents réels d'une entreprise, s'assurer de l'autorisation de celle-ci pour un usage « dans l'enseignement » et procéder si besoin au «démarquage » du document.

Le dossier documentaire est présenté par une table des matières automatisée sur la page de garde, indiquant de la façon la plus claire possible la nature des documents proposés. Il est préférable que chaque sous-partie du dossier documentaire corresponde à chaque dossier du sujet. On prévoira éventuellement une partie documentaire commune à l'ensemble des dossiers (un cahier des charges par exemple).

Au sein d'une mission, il appartient à la candidate ou au candidat de déterminer quels sont les documents utiles pour répondre aux différentes questions qui lui sont posées. Pour autant, il est préférable qu'ils suivent un ordre logique au regard du questionnement.

Lorsque la documentation comporte des éléments de code, il est nécessaire d'en proposer une écriture qui gomme, autant que faire se peut, les spécificités du langage de programmation utilisé. Les éléments spécifiques doivent être commentés, notamment l'usage des fonctions prédéfinies ou des cadres applicatifs (*frameworks)*.

Rédaction des éléments de corrigé

Des éléments de corrigé doivent être fournis avec le sujet. La rédaction des éléments de corrigé au fur et à mesure de l'élaboration du sujet permet aux auteurs de s'assurer de la qualité du questionnement, de sa clarté et de sa faisabilité.

Les éléments de corrigé, le cas échéant, comportent la présentation des alternatives possibles, des autres solutions à admettre. Ils témoignent de la pertinence de la proposition de sujet pour évaluer les compétences, de sa cohérence, de sa compatibilité avec la durée de l'épreuve ; à ce stade, ces éléments ne constituent pas un guide de correction.

Ils comportent également le relevé des sous-compétences dont l'évaluation est prévue par le sujet (pages 43 à 48 du référentiel, reprises en annexe 2).

Proposition de barème

Un barème est à fournir à titre indicatif. Il indique la répartition des points par dossier au prorata du temps nécessaire pour répondre à chaque partie du sujet.

Il n'est pas demandé de fournir un barème détaillé.

Le nombre total de points à répartir est de 100.

Modalités de présentation et de transmission du sujet et des éléments de correction

Les documents produits doivent respecter les règles suivantes :

- **Ne jamais mentionner le nom du diplôme ou de l'épreuve ni dans le sujet ni dans le corrigé** ; ces éléments seront ajoutés par le rectorat en charge du sujet au moment de la duplication.
- Le sujet comme le corrigé doivent être présentés selon **le modèle fourni, en respectant les styles**.
- Le sujet **ne doit pas dépasser 17 pages**, dossier documentaire compris.
- Préférer les formats « .odt » ou « .docx » pour le texte.
- Mentionner le ou les logiciels utilisés pour les éléments non textuels insérés dans le sujet et fournir ces éléments sous forme de fichiers indépendants dans leur format d'origine.
- Utiliser les niveaux de gris pour les images insérées mais fournir les images d'origine avec le sujet.

L'archive fournie à la DEC doit comprendre l'ensemble des fichiers source des documents insérés dans le sujet comme dans le corrigé.

L'annexe 3 présente les recommandations de mise en forme des documents et d'usage de la langue française.

L'annexe 4 liste les conventions concernant les modèles et les schémas.

Annexe 1 : guide pour le recueil d'informations sur le contexte de l'organisation

Les items proposés ci-dessous visent à aider les auteurs dans le recueil d'informations auprès de la ou les organisations qui seront support du cas élaboré. Il ne s'agit pas de collecter de manière exhaustive des informations correspondant à tous les items demandés mais de disposer d'une trame pour la conduite d'entretiens au sein de l'organisation choisie.

Les descripteurs (ressources et relations) du référentiel d'activités professionnelles pour le domaine d'activité "Cybersécurité des services informatiques" constituent aussi un guide pertinent.

Présentation de l'organisation cliente

- Nom de l'organisation
- Secteur d'activité
- Type d'organisation (statut juridique, établissement public ou privé…)
- Taille de l'organisation :
    - Volume d'affaires (chiffre d'affaires, nombre de clients, nombre de produits ou services dans son catalogue…)
    - Effectif du personnel et structure des qualifications
    - Implantation géographique (régionale, nationale, européenne, etc.)
    - Répartition du volume d'affaires
    - Activités à l'étranger
- Évolution récente de l'organisation (historique rapide) et situation sur son marché (leader, challenger, etc.)
- Explicitation d'une problématique ou d'un projet de l'organisation cliente, qui pourra constituer le fil conducteur du sujet
- Événements de sécurité redoutés ou subis par l'organisation, sources et cibles potentielles d'attaques (acteurs, données, applications, services, infrastructures, etc.)
- Relations avec des acteurs administratifs et associatifs lors de problèmes de sécurité : police, justice, CNIL, ANSSI, etc.

Présentation de l'organisation prestataire

- Présentation du prestataire informatique : DSI ? Prestataires externes ?
- Dans quels types de prestations informatiques est-il spécialisé ?
- Dans quelles technologies ?
- Auprès de quels clients ?

- Quels référentiels de bonnes pratiques sont adoptés (au moins en partie, lesquels) ?
- Quel(s) (types de) contrat(s) lient l'organisation cliente et l'organisation prestataire ?

Renseignements propres au système d'information : Système d'information = système informatique + ressources humaines + procédures/méthodes

- Nombre d'utilisateurs du système informatique
- Nombre de personnes dédiées à la gestion du système d'information dans l'organisation
- Statuts et compétences de ces personnes (salariés, intérimaires, régies, etc.)
- Recueil des utilisateurs, habilitations, privilèges et droit d'accès
- Applications utilisées :
    - Applications génériques (bureautique, messagerie, etc.)
    - Applications support (sites collaboratifs, réseaux sociaux d'entreprise, intranets, gestion des ressources humaines, comptabilité, etc.)
    - Applications métiers (progiciels, applications spécifiques)
- Quel arbitrage dans le choix des applications ? (spécifique vs standard, libre vs propriétaire, PGI, etc.)
- Architecture du réseau (articulation LAN, WAN)
    - Systèmes d'exploitation utilisés (environnements Windows, Linux, autres) et utilisations
    - Nombre d'hôtes dans le réseau
    - Nombre de serveurs
    - Quels services sur quels serveurs ?
    - Interconnexions avec d'autres systèmes d'information (lesquels ? Pour quels usages ?)
- Le système informatique est-il partiellement ou totalement externalisé ? Si oui, dans quels domaines ?
- Le système informatique est-il partiellement ou totalement en mode hébergé ?
- Le système informatique fait-il appel à des services de type SaaS, PaaS, IaaS,... ?
- L'organisation est-elle présente sur le *Web* ? Pour quels usages ?
- Quels sont les services mutualisés dans l'organisation (impression, SIRH, etc.) ?
- Quels sont les domaines de gestion les plus directement concernés par les projets de système d'information ?
- Quelles sont les pratiques mises en œuvre pour assurer la sécurité du système d'information, tant au niveau de l'infrastructure que des applicatifs ?

Processus

- L'organisation (cliente ou prestataire informatique) a-t-elle mis en place un management des processus ?
- Quels sont les processus en place ?
- Quels sont les processus métiers (que l'on peut identifier) ?
- L'organisation a-t-elle documenté ses processus ? Selon quelle méthode ? Dispose-t-on d'un exemple ?

Projet de système d'information

- Outils et méthodes de gestion de projet utilisés par l'organisation (planification, gestion du changement, rédaction de cahier des charges,...) ?
- L'organisation a-t-elle des projets système d'information en cours ? Prévus ?
- L'organisation fait-elle une analyse de risque au démarrage de chaque projet ?
- Comment l'organisation prend-elle en compte la sécurité dans les environnements de développement, de test et de production, aussi bien pour les solutions applicatives que pour les solutions d'infrastructure ?
- Présentation des contraintes (contexte concurrentiel, réglementaire, humain, technique, etc.) à l'origine d'un projet d'intervention sur le système d'information
- Présentation des projets (développement d'un nouveau service, besoins de se réorganiser, etc.) qui justifient les besoins en services informatiques.
- Présentation d'un problème de sécurité (anticipé ou effectif) qui nécessite sa prise en charge (celle-ci pouvant prendre la forme d'un projet).
- Comment l'organisation priorise-t-elle un projet par rapport à un autre ?
- Pour un projet
    - Quel est l'état d'avancement du projet ?
    - Quelle est la planification actuelle du projet ?
    - Quel est le budget alloué au projet ?
    - Quels sont les gains attendus par le projet (qualitatifs, quantitatifs) ?
    - Qui a la responsabilité de l'évaluation de ces gains (avant et après le projet) ?
- Dans le cas de projets dédiés à des utilisateurs externes à l'organisation, combien d'utilisateurs le projet est-il censé concerner ?

Annexe 2 : extrait du référentiel de compétences

Bloc de compétences n°3 - Cybersécurité des services informatiques

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités pour répondre aux besoins de sécurité des services informatiques d'une organisation cliente notamment au regard du développement des menaces et attaques en provenance du cybermonde et des risques liés aux usages numériques. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.

La personne titulaire du diplôme participe à la mise en œuvre de l'environnement technologique nécessaire à la sécurité des services informatiques.

Ressources

- Description de l'organisation cliente : son métier, le caractère sensible des activités conduites, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et ses référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité et de sûreté.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre de la mise à disposition d'un service sécurisé.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges fourni par l'organisation cliente : spécifications fonctionnelles et éventuellement techniques, définition du périmètre d'intervention, exigences en termes de protection des données, des applications et des équipements.

Degré d'autonomie, responsabilités

La personne titulaire du diplôme participe à la mise en œuvre de la politique de gestion de la sécurité informatique de l'organisation cliente, en veillant à documenter ses actions. Elle travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation. Elle participe notamment à l'information et à la sensibilisation des utilisateurs aux risques en recommandant les pratiques adaptées. Elle contribue à la sécurisation des accès aux services informatiques : protection des accès aux ressources numériques, aux données, aux équipements et aux applications. En fonction de sa spécialité, elle intervient plus particulièrement sur la sécurité des infrastructures ou des développements d'application.
Dans une petite structure, elle peut travailler en autonomie en tenant compte des risques spécifiques identifiés pour l'organisation cliente. Elle prend en charge l'information, la sensibilisation et la formation des utilisateurs aux questions de sécurité informatique.

Dans une structure plus importante, elle travaille au sein d'une équipe en rendant compte de ses activités.

Compétences	Indicateurs de performance	Savoirs associés
Protéger les données à caractère personnel ▪ Recenser les traitements sur les données à caractère personnel au sein de l'organisation ▪ Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel ▪ Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel ▪ Sensibiliser les utilisateurs à la protection des données à caractère personnel	La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur. La charte informatique contient des dispositions destinées à protéger les données à caractère personnel. Des supports de communication pertinents sont accessibles et adaptés aux utilisateurs. Le recensement des traitements des données à caractère personnel est exhaustif. Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données à caractère personnel en tenant compte des risques identifiés.	<u>Savoirs technologiques</u> Typologie des risques et leurs impacts. Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve. Sécurité et sûreté : périmètre respectif. Sécurité des terminaux utilisateurs et de leurs données : principes et outils. Authentification, privilèges et habilitations des utilisateurs : principes et techniques. Gestion des droits d'accès aux données : principes et techniques. Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique. Protection et archivage des données : principes et

Préserver l'identité numérique de l'organisation ▪ Protéger l'identité numérique d'une organisation ▪ Déployer les moyens appropriés de preuve électronique	L'identité numérique de l'organisation est protégée en s'appuyant sur des moyens techniques et juridiques. La preuve électronique est déployée de manière sécurisée et dans le respect de la législation.	techniques. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications *Web* : risques, menaces et protocoles. Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique. <u>Savoirs économiques, juridiques et managériaux</u> Les données à caractère personnel : définition, réglementation, rôle de la CNIL. L'identité numérique de l'organisation : risques et protection juridique. Droit de la preuve électronique. La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique. Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise. Obligations légales de notification en cas de faille de sécurité. Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions. Les organisations de lutte contre la cybercriminalité.
Sécuriser les équipements et les usages des utilisateurs ▪ Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter ▪ Identifier les menaces et mettre en œuvre les défenses appropriées ▪ Gérer les accès et les privilèges appropriés ▪ Vérifier l'efficacité de la protection	Des supports de communication interne sont accessibles aux utilisateurs et adaptés à leurs destinataires. Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées : - l'accès physique au terminal et à ses données est sécurisé ; - les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ; - les flux réseaux sont identifiés et sécurisés. Les accès et privilèges respectent les règles organisationnelles : - les utilisateurs sont authentifiés ; - les habilitations sont configurées ; - l'accès aux données est contrôlé ; - les privilèges sont restreints. L'efficacité de la protection mise en œuvre est évaluée.	
Garantir la disponibilité, l'intégrité et	Les risques associés à l'utilisation malveillante	

la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques ▪ Caractériser les risques liés à l'utilisation malveillante d'un service informatique ▪ Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité ▪ Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation ▪ Organiser la collecte et la conservation des preuves numériques ▪ Appliquer les procédures garantissant le respect des obligations légales	d'un service informatique sont caractérisés. Les conséquences des actes malveillants sur un service informatique sont identifiées. Les obligations légales en matière d'archivage et de protection des données sont identifiées et respectées. Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation. Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées : - un schéma présentant la segmentation du réseau est disponible ; - les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ; - l'authentification et la confidentialité des échanges sont vérifiées ; - la sécurité de l'administration est prise en compte ; - les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ; - les accès aux données sont contrôlés à chaque étape d'une transaction ; - les systèmes et les applications sont actualisés en fonction des alertes de sécurité ; - les vulnérabilités connues sont contrôlées.	

Option SISR **Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service** ▪ Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique ▪ Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure ▪ Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité ▪ Prévenir les attaques ▪ Détecter les actions malveillantes ▪ Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures	Les dispositifs participant à la disponibilité sont validés (les éléments critiques sont résilients, la charge est répartie efficacement, la qualité des services sensibles est assurée). Les failles potentielles sont identifiées grâce à une activité de veille sur les vulnérabilités. Les bonnes pratiques de sécurité sont prises en compte. Les éléments de sécurité de l'architecture sont conformes et documentés. Les exigences de sécurité sont prises en compte dans le projet de mise en en œuvre d'une solution d'infrastructure. Les dispositifs de détection et de protection des attaques sont opérationnels. Les processus de résolution d'un incident ou d'un problème sont respectés. Le compte rendu d'intervention est clair et explicite. Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité Les contre-mesures sont documentées de manière à en assurer le suivi. La communication écrite et orale est adaptée à l'interlocuteur.	<u>Savoirs technologiques</u> Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards. Cybersécurité : bonnes pratiques, normes et standards. Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services. Outils de sécurité : prévention et détection des attaques, gestion d'incidents. <u>Savoir économique, juridique et managérial</u> Responsabilité civile et pénale de l'administrateur système et réseau.

Option SLAM **Assurer la cybersécurité d'une solution applicative et de son développement** ▪ Participer à la vérification des éléments contribuant à la qualité d'un développement informatique ▪ Prendre en compte la sécurité dans un projet de développement d'une solution applicative ▪ Mettre en œuvre et vérifier la conformité d'une solution applicative et de son développement à un référentiel, une norme ou un standard de sécurité ▪ Prévenir les attaques ▪ Analyser les connexions (logs) ▪ Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures	Le respect des bonnes pratiques de développement informatique est vérifié (les structures de données sont normalisées, les accès aux données sont optimisés, le code est modulaire et robuste, les tests sont effectués). Les préoccupations de sécurité sont prises en compte à toutes les étapes d'un développement informatique. Les bonnes pratiques de sécurité sont mises en œuvre à toutes les étapes d'un développement informatique. Des tests de sécurité sont prévus et mis en œuvre. Les traitements sur les données à caractère personnel sont déclarés et respectent la réglementation. Le système d'authentification est conforme aux règles de sécurité. L'accès aux données respecte les règles de sécurité. Les échanges de données entre applications sont protégés. Les composants utilisés sont certifiés, sécurisés et actualisés. Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité. Les contre-mesures sont documentées de manière à en assurer le suivi. La communication écrite et orale est adaptée à l'interlocuteur.	<u>Savoirs technologiques</u> Développement informatique : méthodes, normes, standards et bonnes pratiques. Aspects réglementaires du développement applicatif : protection de la vie privée dès la conception, protection des données par défaut, sécurité par défaut, droit des individus. Sécurité du développement d'application : gestion de projet, architectures logicielles, rôle des protocoles, authentification, habilitations et privilèges des utilisateurs, confidentialité des échanges, tests de sécurité, audit de code. Vulnérabilités et contre-mesures sur les problèmes courants de développement. Environnements de production et de développement : fonctionnalités de sécurité, techniques d'isolation des applicatifs. <u>Savoir économique, juridique et managérial</u> Responsabilité du concepteur de solutions applicatives.

Annexe 3 : recommandations de mise en forme et d'usage de la langue française

Respect des règles de la langue française

On veillera à s'adresser systématiquement aussi bien à une candidate qu'à un candidat.

L'utilisation de la terminologie officielle française est toujours requise[6]. L'emploi d'une terminologie spécifique à tel ou tel matériel ou logiciel doit être effectué avec prudence :

- Les noms de marque, d'outil ou de langage doivent être évités ; leur usage doit se limiter aux cas où ils sont nécessaires à la compréhension ou à la résolution du sujet. Les termes génériques seront préférés (par exemple « fournisseur d'accès à internet» plutôt que le nom du fournisseur).
- **Les expressions anglo-saxonnes doivent être les moins nombreuses possibles, toujours traduites en français, éventuellement présentées ensuite entre parenthèses et en italiques,** par exemple mobile multifonction (*smartphone*).
- À leur première utilisation dans le texte, les termes techniques sont exprimés en français suivis du sigle anglais. Par exemple : réseau privé virtuel (*Virtual private network - VPN*) ; dans la suite du texte réseau privé virtuel (*VPN*). Quand le sigle est un nom de protocole ou de langage, il peut être utilisé tel que : langage *SQL*, protocole *HTTP*.

Respect des règles de mise en forme d'un document

- Les noms de marque, de société ou encore les références aux objets techniques seront présentés en italiques (ex : *MySQL, Windows, Web*, *Java, PHP,* mais aussi nom de logiciel ou de fichier *consulterFactures.php*).
- L'usage des majuscules dans la langue française est limité. L'emploi des minuscules est requis sauf dans les cas suivants : à la première lettre de chaque phrase, la première lettre des noms propres, et les sigles. Cette règle est également applicable aux titres de documents et de chapitres.
- En début de phrase, les majuscules doivent être accentuées quand elles correspondent par exemple aux caractères é (É), à (À).
- Les noms des organisations clientes et prestataires sont en caractères droits et respectent la règle générale concernant l'usage des majuscules.
- Les sigles doivent être explicités à leur première citation dans le sujet.
- Il convient d'écrire de la même manière les sigles et les acronymes, en majuscules et sans points séparatifs entre les lettres (exemple SARL). Cependant, lorsqu'un sigle de plus de trois lettres peut être lu de façon syllabique, il est écrit en minuscules (sauf la première lettre) : Certa, Unesco. Un sigle peut combiner les deux : *MySQL*, *AmatsiDBI*, *Gest-Music Gest-PC*. Attention, dans les articles récents, on trouve *VLAN* pour *virtual LAN* avec la règle des trois lettres mais aussi *Vlan* avec la règle des plus de trois lettres.

[6] Pour les traductions, utiliser le site http://www.culture.fr/Ressources/FranceTerme/Librairie

- Les conventions typographiques en usage à l'imprimerie nationale relatives aux énumérations sont recensées à l'adresse suivante : http://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Conventions_typographiques#Listes_verticales. Ainsi, si les items ne sont pas des phrases, il convient d'utiliser le point-virgule après chaque item de l'énumération et un point après le dernier item. Dans le cas d'énumérations imbriquées, il convient d'utiliser le point-virgule pour les items de niveau 1, virgule pour les items de niveau 2 et une lettre minuscule au début de chaque item.

Annexe 4 : convention concernant les modèles et schémas

Les candidats sont libres d'utiliser les modèles de leur choix pour représenter les données, les traitements, les processus, les algorithmes, les programmes. Il peut leur être demandé d'indiquer sur la copie le formalisme choisi et de s'y tenir : il ne s'agit pas de mélanger différents formalismes au sein d'un même schéma.

Les schémas et les éléments de langages fournis dans le sujet doivent être les plus communément utilisés.

Quand il s'agit d'analyser l'organisation des données, l**es représentations graphiques (**diagramme de classe, schéma entité-association ou encore schéma relationnel) **sont privilégiées** car elles sont plus faciles à lire et à interpréter. Lorsque la dimension conceptuelle est interrogée, la représentation sous forme de diagramme de classe et de schéma entité-association est à privilégier. Dans le cas d'un questionnement lié à la manipulation d'une base de données, le schéma relationnel est à présenter, notamment en version textuelle.

Les langages de programmation les plus couramment utilisés sont Java, PHP, C#. On veillera à ne pas utiliser de caractères accentués dans le code.

Toutes les indications nécessaires pour interpréter correctement la sémantique d'un schéma ou d'un élément de programme sont portées dans le sujet (signification des variables, des attributs, des clés étrangères, des équipements, etc.). Pour les schémas, une légende est incluse au besoin. Les programmes sont commentés en italiques.

Il convient de **ne pas utiliser de couleurs** dont l'interprétation serait nécessaire pour comprendre un schéma, en effet les sujets sont toujours dupliqués en noir et blanc.

Conventions pour l'écriture textuelle du schéma relationnel, si elle est utilisée

- Il n'y a pas de blanc ni de caractère accentué dans les noms de table ou d'attribut.
- Chaque nom de table commence par une majuscule et est suivi de minuscules. S'il est composé de plusieurs mots, ceux-ci sont collés et distingués par une majuscule. Pour des raisons de lisibilité, le nom des tables est écrit en caractères gras.
- Chaque nom d'attribut est écrit en minuscule. S'il est composé de plusieurs mots, ils sont collés et distingués par une majuscule. Le nom choisi pour l'attribut figure le rôle de son domaine dans la relation.
- On privilégiera « id » comme nom d'attribut identifiant d'une relation ou « code » ; « numero » sera utilisé uniquement si il s'agit d'un champ numérique (cependant une approche par le rôle est à privilégier à une approche par le type).
- Une clef étrangère porte un nom significatif de son rôle dans la table.

Exemple :

Etablissement (id, nom, adresseRue, codePostal, ville, tel, adresseElectronique, type)
Clé primaire : id

TypeChambre (id, libelle)
Clé primaire : id

Offre (idEtab, idTypeChambre, nombreChambres)
Clé primaire : idEtab, idTypeChambre
Clés étrangères : idEtab en référence à id de Etablissement
idTypeChambre en référence à id de TypeChambre

Groupe (id, nom, identiteResponsable, adressePostale, nombrePersonnes, nomPays, hebergement)
Clé primaire : id

Attribution (idEtab, idTypeChambre, idGroupe, nombreChambres)
Clé primaire : idEtab, idTypeChambre, idGroupe
Clés étrangères : idEtab, idTypeChambre en référence à idEtab, idTypeChambre de Offre
idGroupe en référence à id de Groupe

Annexe 5 : demande d'autorisation d'utilisation d'informations

AUTORISATION D'UTILISER DES INFORMATIONS DANS LE CADRE DE LA CONCEPTION D'UN SUJET

Je soussigné(e)

Nom : _____

Prénom : _____

Représentant(e) légal(e) de la société ou organisme

Dénomination :
(cachet)

Détenteur (détentrice) des droits sur la ou les marques suivantes :

Autorise l'utilisation
Du nom de la société
OUI NON
De la ou les marque(s) suivante(s) :

Autorise l'utilisation et l'adaptation des informations fournies à l'équipe d'auteurs
OUI NON

S'engage à ne pas divulguer le fait d'avoir communiqué des informations à une équipe de conception de sujet, et ce jusqu'à la sortie du sujet et pendant 5 ans si le sujet n'est pas retenu dès la session en vigueur (les auteurs sont tenus au secret professionnel pour toutes les informations collectées à l'occasion de leur travail.)

Date :

Signature manuscrite Tampon de l'organisation