Corrigé

Barème

DOSSIER A : Participation à l'atelier d'analyse de risques		**12 points**
DOSSIER B : Amélioration de l'authentification		**26 points**
DOSSIER C : Validation des demandes client		**24 points**
DOSSIER D : Envoi des données de demande au PGI		**18 points**
	TOTAL	**80 points**

Dossier A – Participation à l'atelier d'analyse de risques

Mission A1 – Les enjeux de sécurité

Question A1.1
Proposez une évaluation des quatre critères de sécurité pour les cas d'utilisation n°2 et 6.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et 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.

Excellente maîtrise		7 à 8 critères sont correctement évalués
Bonne maîtrise		5 à 6 critères correctement évalués
Maîtrise partielle		De 1 à 4 critères correctement évalués
Non maîtrisé		Tous les critères sont faux.
Non évaluable		Non répondu.

Cas N°	Cas d'utilisation	Critères de sécurité			
2	Un client consulte le catalogue des pièces	Confidentialité :	+	Intégrité :	++
		Disponibilité :	+	Preuve :	0
6	Le client signe électroniquement les documents	Confidentialité :	++	Intégrité :	++
		Disponibilité :	++	Preuve :	++

Cas n° 2 : pour les critères confidentialité et disponibilité, on acceptera ++, pour le critère Intégrité on acceptera +.

Mission A2 – Les événements redoutés et les mesures à prendre

Question A2.1
Évaluez l'impact métier correspondant aux événements redoutés n°4 et 5.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité

Excellente maîtrise		Un impact correct par évènement
Bonne maîtrise		Un impact correct pour un seul évènement.
Non maîtrisé		Tous les impacts sont inadaptés
Non évaluable		Non répondu.

Événement N°	Événement redouté	Impact métier	Gravité
4	Un utilisateur/client peu scrupuleux saisit et valide des demandes de pièces non compatibles avec l'aéronef déclaré en panne.	Épuisement du stock d'équipements pour certaines références > coûts élevés pour les avions immobilisés > perte d'image	++
5	Un attaquant pénètre dans le système PGI par détournement d'une demande de pièce	Compromission des données essentielles de l'entreprise	++

Question A2.2

Proposer deux mesures à prévoir pour chacun des scénarios de risques n°2 et 5.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prendre en compte la sécurité dans un projet de développement d'une solution applicative		
Excellente maîtrise		Deux mesures pertinentes par scénario.
Bonne maîtrise		Deux mesures pertinentes.
Maîtrise partielle		Une mesure pertinente.
Non maîtrisé		Toutes les mesures sont non pertinentes.
Non évaluable		Non répondu.

Événement N°	Scénario de risques	Mesures à prévoir
2	En tant qu'attaquant externe j'utilise un outil d'attaque des mots de passe	-Utiliser une authentification à plusieurs facteurs -Limiter le nombre de tentatives -Bannir l'attaquant avec un déverrouillage possible (code SMS) - politique de mot de passe fort - authentification par certificat
5	En tant qu'attaquant j'essaie de corrompre le PGI par injection de code dans les demandes d'équipements	-Vérifier/filtrer les données de demandes transmises -Appliquer les mises à jour de sécurité recommandées par l'éditeur du PGI -Limiter l'exposition du serveur hébergeant le PGI peut être cité mais n'est pas une mesure suffisante..

Question A2.3
Expliquez ce qui peut amener des clients peu scrupuleux à réaliser les scénarios n° 3 et 4.

Compétence évaluée : Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité		
Excellente maîtrise		Réponse pertinente.
Maîtrise partielle		Réponse mal justifiée.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Une pénurie de certains équipements peut clouer au sol des avions et le coût d'immobilisation est très coûteux. Il peut donc s'agir d'acte de concurrence déloyale provoquant la raréfaction de pièces sensibles.

Cyber-influence L2i (lutte informatique d'influence) domaine de la défense.

Dossier B – Durcissement de l'authentification

Mission B1 – Sécurisation des mots de passe

Question B1.1
Choisir la solution qui semble la plus sécurisée en justifiant votre réponse.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Appliquer les procédures garantissant le respect des obligations légales

Excellente maîtrise		Le candidat propose un algorithme de hachage et justifie son choix.
Bonne maîtrise		Le candidat propose un algorithme de hachage sans justifier son choix.
Non maîtrisé		Le candidat propose de chiffrer le mot de passe.
Non évaluable		Non répondu.

Dans un souci de sécurité il est essentiel de préserver à tout prix la confidentialité des mots de passe. Donc si jamais le contenu de la table contenant les mots de passe était aux mains d'attaquants, il ne faut pas que l'on puisse déchiffrer ces mots de passe, d'où la nécessité d'utiliser un algorithme de hachage, par nature non réversible. La vérification consiste donc à hacher le mot de passe reçu par le formulaire de login et à le comparer à la version stockée dans la base de données.

Question B1.2
Expliquer l'importance d'ajouter un grain de sel (salage) lors de l'opération de hachage.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Appliquer les procédures garantissant le respect des obligations légales

Excellente maîtrise		L'explication du candidat est pertinente et cite les attaques par rainbow table
Bonne maîtrise		L'explication du candidat est pertinente mais ne cite pas les attaques par rainbow table.
Non maîtrisé		L'explication est non pertinente.
Non évaluable		Non répondu.

Le salage permet de renforcer la sécurité car il permet d'obtenir une chaîne hachée différente pour deux mots de passe identiques. Les attaques par rainbow table (arc en ciel) deviennent quasiment impossibles à mettre en œuvre.

Mission B2 – Prévention des injections de code SQL

Question B2.1
Modifier le code de la méthode *readByLogin* de la classe ClientDao afin d'éviter les injections *SQL*.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prévenir les attaques		
Excellente maîtrise		Le candidat maîtrise les 3 niveaux : • requête SQL adaptée • Préparation et valorisation du paramètre • Exécution et récupération des données
Bonne maîtrise		Le candidat maîtrise 2 des 3 niveaux
Maîtrise partielle		Le candidat maîtrise 1 seul des 3 niveaux
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

```
1.  class ClientDao extends Dao
2.  {
3.      public function readByLogin($login):?Client
4.      {   // renvoie un Client ou null si aucun login ne correspond
5.          $connex = DB::getPdo();
6.          $req = 'SELECT id, nom, login, pass, courriel, telephone, adresse,
7.              pays, estBloque, codePinOtp FROM client WHERE login = ?';
8.          $res = $connex->query($req);
9.          $prep = $connex->prepare($req);
10.         $prep->bindValue(1, $login, PDO::PARAM_STR);
11.         $prep->execute();
12.         $enreg = $prep->fetch(PDO::FETCH_OBJ);
13.         if ($enreg != false) {
14.             $unClient = new Client($enreg->id, $enreg->nom, $enreg->login, $enreg->pass,
15.             $enreg->courriel, $enreg->telephone, $enreg->adresse, $enreg->pays,
16.             $enreg->estBloque, $enreg->codePinOtp);
17.         } else {
18.             return null;
19.         }
20.         $res->closeCursor();
21.         return $unClient;
22.     }   //autres méthodes du DAO...
23. }
}
```

Mission B3 – Authentification à deux facteurs et journalisation des connexions

Question B3.1
Proposer à l'équipe de développement deux autres solutions d'authentification à deux facteurs, sans préciser la mise en œuvre.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prendre en compte la sécurité dans un projet de développement d'une solution applicative		
Excellente maîtrise		Le candidat propose au moins deux solutions
Maîtrise partielle		Le candidat propose une seule solution.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Il s'agit de combiner plusieurs techniques d'authentification entre les 3 formes :

- mémorielle qui représente une chose que l'intéressé connaît **(un secret)**,
- matérielle qui se réfère à quelque chose qu'il possède **(un objet)**,
- corporelle qui utilise un trait physique de l'utilisateur **(une biométrie)**.

En complément du login / mot de passe on peut trouver :

- Un code unique envoyé par SMS ou par mél ;
- Une application d'authentification ou une clé cryptographique ;
- Une reconnaissance vocale, faciale ou par empreinte digitale ;
- Obtenir des codes de validation avec des authentificateurs (Microsoft Authenticator, Google Authenticator,…)

Evidemment on ne peut demander au candidat de tout citer, mais 2 propositions au moins.

Question B3.2
Modifier le code de la vue *loginView.php* pour permettre la saisie du mot de passe à usage unique (clé *OTP*).

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • 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		
Excellente maîtrise		La ligne HTML est correcte.
Bonne maîtrise		La balise <input> est présente avec ses 2 attributs type et name
Maîtrise partielle		La balise <input> est présente mais non complète.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

loginView.php

```
…
  <form method="post" action="/login/val" enctype="multipart/form-data">
     <label for="login">Login :</label><input type="text" id="login" name="login" />
     <label for="pass">Mot de passe :</label><input type="password" id="pass" name="pass" />
     <label for="code_otp">Code de validation :</label><input type="text" id="code_otp"
name="code_otp" />
     <input type="submit" value="Valider">
  </form>
…
```

Question B3.3
Écrire le code nécessaire dans la méthode *verifLogin* de la classe LoginCtrl pour vérifier la clé *OTP* saisie et pour écrire dans le fichier journal (*logs*).

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Analyser les logs (cf. guide d'accompagnement inclut la journalisation des accès)		
Excellente maîtrise		Le candidat maîtrise les 4 niveaux : 1. Récupération et filtrage du code otp saisi 2. Génération de la clé OTP 3. Contrôle de concordance et log OK 4. log de non concordance
Bonne maîtrise		Clé OTP mal gérée mais écriture dans les logs bien gérée.
Maîtrise partielle		La logique est présente mais le code est très incomplet.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

class LoginCtrl {

```
    ...
    //méthode appelée pour vérifier le login d'un utilisateur
public function verifLogin() {

        $loginForm = filter_input(INPUT_POST, 'login', FILTER_SANITIZE STRING);
        $passForm = filter_input(INPUT_POST, 'pass', FILTER_SANITIZE STRING);
        $otpForm = filter_input(INPUT_POST, code_otp, FILTER_SANITIZE INT);

        $daoC = new ClientDao();
        $client = $daoC->readbyLogin($loginForm);

        $otp = new OTP($client);
        $code = $otp->getCode(new DateTime());

        if (password_verify ($passForm , $client->getPass()) && $otpForm == $code ) {
            syslog(LOG_INFO, 'Connexion client ' . $client->getId());
            new AccueilView();
        } else {
            $message = 'pass';
            if ( $otpForm != $code ) {
                $message = 'otp';
            }
            syslog(LOG_WARNING, 'Erreur connexion client  login ' . $loginForm . ' cause : '
. $message);
            new LoginView("Authentification invalide");
        }
   }
}
```

Dossier C – Validation des demandes client

Mission C1 – Envoi des documents au client et signature du contrat

Question C1.1
Indiquer la condition nécessaire pour que cette solution d'échange électronique soit recevable devant les tribunaux en cas de contestation par le client.

Compétence évaluée :
Préserver l'identité numérique de l'organisation
- Déployer les moyens appropriés de preuve électronique

Excellente maîtrise		Le candidat mentionne la signature électronique et l'organisme agréé
Bonne maîtrise		Le candidat mentionne uniquement la signature électronique
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Selon le Code Civil un message électronique peut avoir la même valeur juridique qu'un courrier manuscrit s'il est certifié, c'est-à-dire qu'il comporte une signature électronique. Pour être conforme, elle doit être réalisée par un organisme agrée et être sécurisée. Dans ce cas-là, le courriel ou message électronique fait foi.

Question C1.2
Indiquer les solutions techniques à mettre en œuvre pour répondre à chacune des quatre exigences. Chaque exigence devra être traitée de façon indépendante.

Compétence évaluée :
Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques
- Appliquer les procédures garantissant le respect des obligations légales

Excellente maîtrise		Chacun des 4 points est bien traité
Bonne maîtrise		3 points sont bien traités
Maîtrise partielle		1 seul point est bien traité
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

1. une totale confidentialité des échanges ;

   Solution : chiffrer le contenu du message lui-même car quand 2 serveurs SMTP communiquent, il n'est pas garanti que la communication soit chiffrée par TLS.

   On accordera les points aux candidats qui mentionnent simplement une communication chiffrée (TLS).

2. la preuve que les documents sont authentiques et non modifiés ;

   Solution : Utiliser une signature numérique

3. la preuve que le client a bien reçu les documents ;

   Pas de solution complète mais quelques pistes :
   - L'accusé de réception n'est pas satisfaisant car le destinataire n'a pas l'obligation de l'utiliser.

- L'envoyeur peut déposer le document sur un espace sécurisé et fournir les identifiants de connexion au destinataire. L'envoyeur peut ensuite suivre les actions de destinataire et détruire le document une fois téléchargé.

4. la signature du client qui l'engage légalement.

Solution : Utiliser une signature numérique, celle-ci est construite à partir de la clé privée : seul son possesseur est donc en capacité de signer un document en son nom.

Mission C2 – Gestion des clients abusifs

Question C2.1
Écrire la requête qui permet d'obtenir la liste des clients ayant des demandes de plus de 24 heures non confirmées. Pour chaque client on souhaite afficher l'identifiant, le nom et le nombre total de pièces demandées.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement
- Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures

Excellente maîtrise		La requête est correcte.
Bonne maîtrise		La requête est partiellement correcte : manque une restriction sur les dates ou jointure manquante.
Maîtrise partielle		Absence du GROUP BY
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

```
SELECT client.id, nom, COUNT(*) AS nb_demandes_non_val
FROM demande
JOIN client ON idClient = client.id
WHERE dateConfirmation IS NULL
AND dateDemande < NOW() - INTERVAL 1 DAY
GROUP BY client.id, nom
```

Question C2.2
Ecrire le code du déclencheur *(trigger)* qui permet d'obtenir cette fonctionnalité.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures		
Excellente maîtrise		Le trigger est bien codé sur 4 niveaux : 1. En-tête du trigger 2. Déclaration et récupération du nombre d'abus en utilisant la fonction fournie 3. condition sur le nombre d'abus 4. requête de mise à jour.
Bonne maîtrise		Le trigger est bien codé mais le nombre d'abus n'est pas correctement récupéré.
Maîtrise partielle		La requête de mise à jour n'est pas réalisée.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

```
CREATE OR REPLACE TRIGGER bannir_abus
BEFORE INSERT ON Demande
FOR EACH ROW
BEGIN
        DECLARE nb int;
        SELECT nb_abus(NEW.idClient) INTO nb;
        IF nb = 2
                UPDATE client
                SET estBloque = true
                WHERE id = NEW.id;
                CALL EXIT;
        ENDIF
END
```

On acceptera une réponse utilisant la syntaxe des langages de tous les SGBD.

Remarque : Il est possible de rajouter un test pour savoir si un client est déjà bloqué (non exigé).

Question C2.3
Adapter la modélisation des données existante pour intégrer la compatibilité des types de pièce avec les modèles d'aéronef.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Analyser des incidents de sécurité, proposer et mettre en œuvre des contre-mesures		
Excellente maîtrise		Le modèle de données proposé intègre : • la suppression de l'attribut modeleAeronef dans l'entité Demande, • la gestion de la compatibilité du type de pièce demandé avec le modèle d'aéronef concerné.
Bonne maîtrise		Seule la gestion de la compatibilité du type de pièce demandé avec le modèle d'aéronef concerné est prise en compte (l'attribut modeleAeronef dans l'entité Demande n'a pas été supprimé)
Maîtrise partielle		L'entité ModeleAeronef n'a pas été ajoutée.
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

Modèle entité association

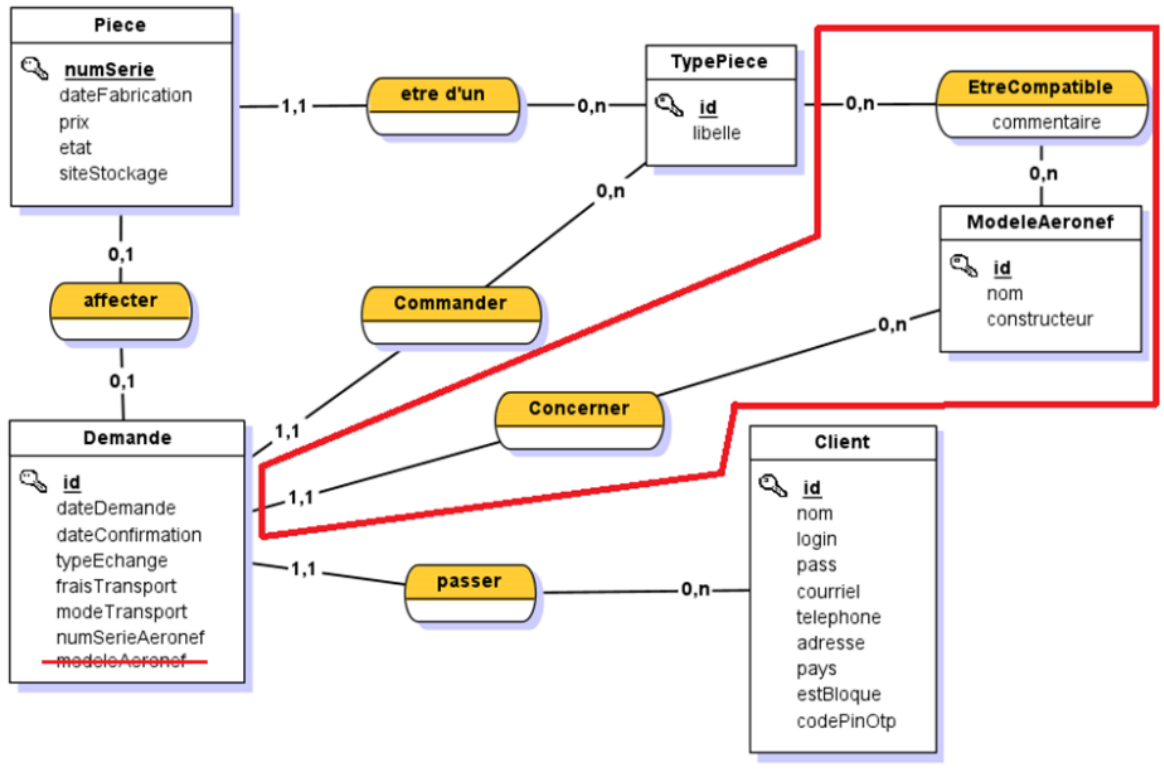
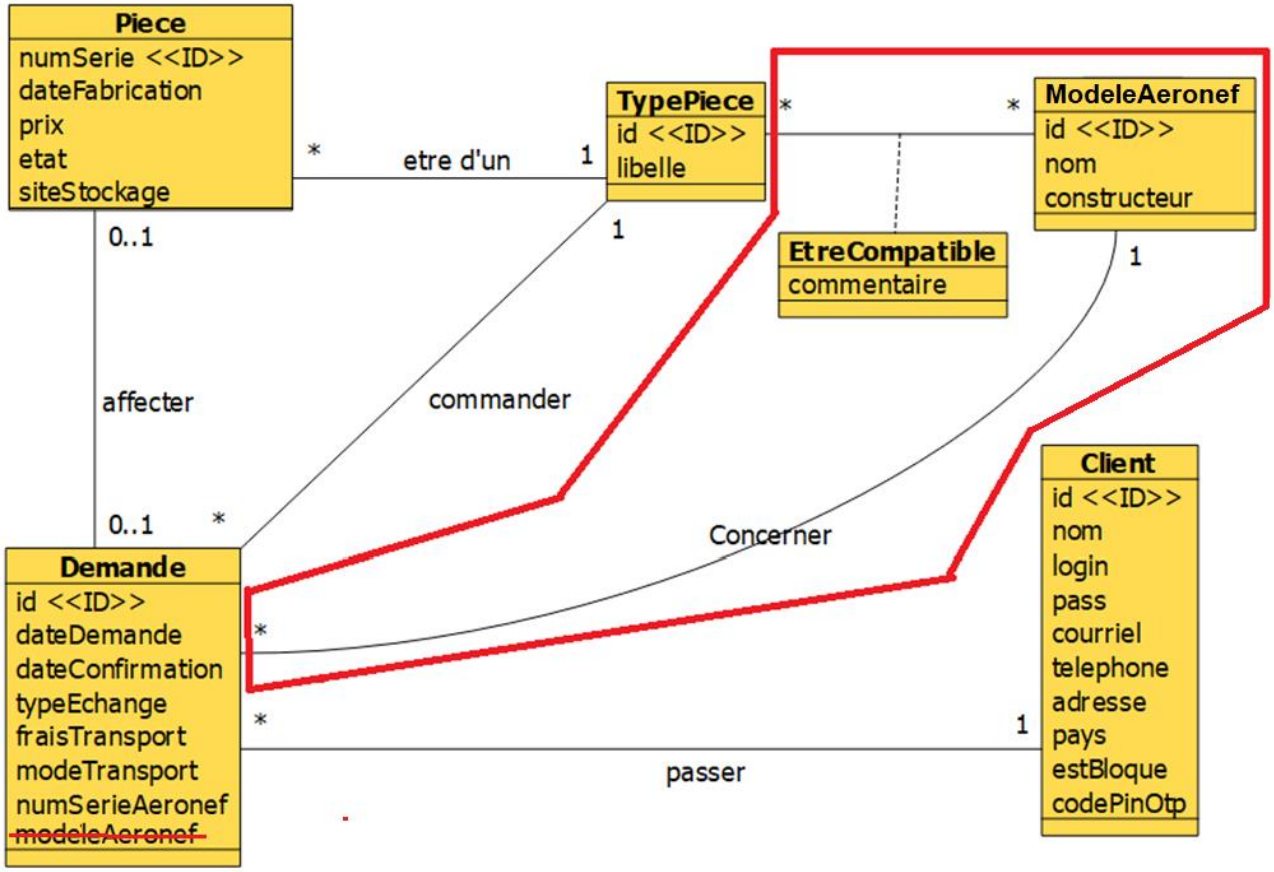


Diagramme de classes



Question C2.4
Proposer une solution pour implémenter cette contrainte métier sans la mettre en œuvre.

Compétence évaluée : Assurer la cybersécurité d'une solution applicative et de son développement • Prévenir les attaques		
Excellente maîtrise		La solution proposée est pertinente (trigger ou interface)
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

- Trigger sur INSERT qui va vérifier la cohérence entre le modèle de l'aéronef et le type de pièce,
- Gestion par l'application grâce à l'interface graphique, par exemple choix d'un type de pièce dans une liste déroulante alimentée uniquement par les types de pièces compatibles avec le modèle de l'aéronef préalablement déclaré.

Dossier D – Envoi des données de demande au PGI

Mission D1 – Finalisation d'une interface de programmation (*API*) de type *REST*

Question D1.1
Réaliser la méthode de l'interface de programmation (API) REST située dans la classe DemandeRest qui permettra d'ajouter une demande.

Compétence évaluée :
Assurer la cybersécurité d'une solution applicative et de son développement

- 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

Excellente maîtrise		La méthode est bien codée en 3 niveaux : 1. Directives et signature 2. Création de la demande 3. Retour de la réponse
Bonne maîtrise		Le retour de la réponse n'est pas correctement géré
Maîtrise partielle		Les directives et la signature sont incorrectes et la demande n'a pas été créée.
Non maîtrisé		Réponse non adaptée.
Non évaluable	**0**	Non répondu.

```
@POST
@Consumes(MediaType.APPLICATION_JSON)
public Response createDemande(DemandeJson laDemandeJson) {

        // le service crée une demande
        boolean result = DemandeService.create(laDemandeJson);

        // result vaut true (demande créée) ou false
        if (result == true) {
                return Response.status(Status.CREATED).build();
        }
        else {
                return Response.status(Status.BAD_REQUEST).build();
        }
}
```

Mission D2 – Contrôle des données

Question D2.1

a) Compléter la méthode *verifDonneesCreate* de la classe DemandeService pour qu'elle contienne les contrôles demandés, en utilisant la grammaire des expressions régulières.

b) Proposer un contrôle supplémentaire permettant de sécuriser davantage la date de la demande. Le code n'est pas demandé.

Compétence évaluée :

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

Excellente maîtrise		Réponse correcte sur a et b
Bonne maîtrise		Une seule réponse a ou b
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

a)

```
if (Pattern.matches("STANDARD|SILVER|GOLD", laDem.getTypeEchange()) == false){
      res = false;
}
```

b) Contrôles possibles :

La date de demande doit être inférieure ou égale à la date du jour

Question D2.2
Compléter le test unitaire manquant de la classe DemandeServiceTest permettant de s'assurer du bon fonctionnement de la méthode *create* de la classe DemandeService.

Compétence évaluée : 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		
Excellente maîtrise		Test correctement codé en 3 niveaux : • Création de la demande avec des valeurs valides • Appel de la méthode create • Appel de la méthode Assert
Bonne maîtrise		La méthode Assert est appelée avec les bons paramètres (teste une valeur true) et les valeurs choisies pour la demande sont valides. Par contre la déclaration de la demande ou l'appel de la méthode create sont absents ou incorrects.
Maîtrise partielle		La méthode Assert teste une valeur false
Non maîtrisé		Réponse non adaptée.
Non évaluable		Non répondu.

```
public class DemandeServiceTest {

	// déclaration d'une demande
	private DemandeJson dem4;

	@Before
	public void setUp(){
		// création d'une demande correcte
		this.dem4 = new DemandeJson(4, "2022-03-23", " ",
				"STANDARD", 0, "INTERNE", 44, "A321", 2, 3, null);

	}
	// test d'une demande correcte
	@Test
	public void testCreateOK(){

		// exécution méthode
		result = DemandeService.create(dem4);

		// test du retour de la méthode
		assertEquals("Create OK", true, result);
	}
}
```