ANALYSE DE RISQUE

BTS SIO Option SLAM — Épreuve E7

L'analyse de risque est une démarche structurée qui permet de prioriser les mesures de sécurité selon la vraisemblance et la gravité des menaces. Elle constitue le socle de toute politique de sécurité applicative, et s'applique dès la phase de conception (user stories / sprint planning) en méthode Agile/Scrum.

0. Sûreté et Sécurité : deux notions distinctes

Ces deux termes sont souvent confondus mais recouvrent des périmètres différents. L'épreuve E7 peut explicitement demander de les distinguer.

	Sûreté (Safety)	Sécurité (Security)
Définition	Protection contre les accidents et défaillances non intentionnelles	Protection contre les actes malveillants intentionnels
Origine du risque	Erreur humaine, panne, catastrophe naturelle, défaut logiciel	Attaque externe, malveillance interne, cyberattaque
Exemples SI	Panne serveur, erreur de saisie, bug critique, coupure réseau	Intrusion, phishing, ransomware, vol de données
Mesures typiques	PRA/PCA, redondance, sauvegardes, tests de charge	Pare-feu, authentification, chiffrement, WAF, IDS
Référentiel	IEC 61508, ISO 25010 (fiabilité)	ISO 27001, EBIOS RM, OWASP, RGPD

> 💡 *En E7, un récit utilisateur peut générer des événements redoutés relevant de la sûreté (ex : perte de données par bug) ET de la sécurité (ex : vol de données par injection SQL). Les deux doivent être traités.*

Les deux approches se complètent autour de la triade CIA enrichie :

- **Disponibilité :** le système fonctionne quand on en a besoin (sûreté + sécurité)
- **Intégrité :** les données ne sont pas altérées, ni par erreur ni par malveillance
- **Confidentialité :** seuls les ayants droit accèdent aux informations (sécurité)
- **Preuve / Traçabilité :** 4ème critère souvent ajouté en E7 — les logs constituent une preuve opposable (voir A1.3)

1. Évaluation des Risques

1.1 La matrice Probabilité × Impact

Un risque se quantifie par deux axes indépendants :

- **Probabilité (vraisemblance) :** à quelle fréquence cet événement pourrait-il survenir ? (1 = rare → 4 = quasi-certain)
- **Impact (gravité) :** quelles seraient les conséquences sur le SI, les données ou l'activité ? (1 = négligeable → 4 = critique)

Niveau de risque = Probabilité × Impact. La matrice à double entrée permet de visualiser et prioriser.

Matrice d'évaluation des risques (Probabilité × Impact)

Probabilité ↓ Impact →	Impact 1 Négligeable	Impact 2 Limité	Impact 3 Important	Impact 4 Critique	Niveau
Quasi-certain					Élevé→Critique
Probable					Moyen→Élevé
Possible					Faible→Moyen
Rare					Faible
	Faible	Moyen	Élevé	Critique	

1.2 Les acteurs à l'origine des menaces (sources de risque)

Tout tableau d'acteurs doit distinguer les menaces internes et externes, intentionnelles et non intentionnelles.

Acteur / Source	Type	Motivations / Causes	Exemples d'actions
Cybercriminel externe	Externe / Intentionnel	Gain financier, espionnage, déstabilisation	Phishing, ransomware, SQLi, DDoS
Concurrent / État	Externe / Intentionnel	Espionnage économique, sabotage	APT, vol de propriété intellectuelle
Employé malveillant	Interne / Intentionnel	Vengeance, appât du gain, idéologie	Exfiltration de données, sabotage de BDD
Employé négligent	Interne / Non intentionnel	Ignorance, erreur, fatigue	Clic phishing, mot de passe faible, mauvaise config
Prestataire / Sous-traitant	Externe-Interne / Variable	Accès légitime mais périmètre non maîtrisé	Accès excessif, faille dans code livré
Script kiddie	Externe / Opportuniste	Curiosité, notoriété	Scan de vulnérabilités, exploits automatisés
Défaillance technique	Environnement / Non intentionnel	Panne, bug, catastrophe naturelle	Crash serveur, coupure réseau, bug applicatif

1.3 Critères DICT — Besoins de sécurité par récit utilisateur

Pour chaque user story, on évalue quatre critères sur une échelle de 0 à 3 (ou Faible / Moyen / Fort) :

Critère	Question posée	Exemples de niveaux
D - Disponibilité	Les utilisateurs ont-ils besoin d'accéder au service en permanence ?	Fort : paiement en ligne | Moyen : rapports mensuels | Faible : page statique
I - Intégrité	Les données doivent-elles être absolument exactes et non altérées ?	Fort : données médicales, transactions | Moyen : catalogue | Faible : avis utilisateurs
C - Confidentialité	Les données sont-elles sensibles ou réservées à certains ?	Fort : données de santé, paiement | Moyen : données clients | Faible : contenu public
T - Traçabilité / Preuve	Faut-il conserver une trace des actions pour audit ou contentieux ?	Fort : transactions financières | Moyen : connexions | Faible : navigation anonyme

▸ Exemple d'évaluation DICT pour deux user stories

User Story	D	I	C	T	Justification synthétique
Connexion au compte client	Fort	Fort	Fort	Fort	Accès critique, données personnelles, risque de fraude, audit de connexion obligatoire
Consultation du catalogue public	Moyen	Moyen	Faible	Faible	Service doit être disponible mais les données sont publiques, intégrité du contenu éditoriale seulement

1.4 Conditions pour qu'un log serve de preuve (A1.3)

Pour qu'un élément de traçabilité soit opposable en cas de contentieux, il doit satisfaire cumulativement :

- **Horodatage fiable et synchronisé :** utilisation d'un serveur NTP de référence — l'heure doit être vérifiable et non contestable
- **Intégrité garantie :** les logs ne doivent pas pouvoir être modifiés après écriture (stockage WORM, hash SHA-256 de chaque entrée, signature numérique)
- **Complétude :** chaque action pertinente est enregistrée : qui (identifiant), quoi (action), quand (timestamp), depuis où (IP)
- **Conservation suffisante :** durée alignée sur la prescription légale applicable (5 ans en droit commercial, plus en cas de données personnelles)
- **Accessibilité et lisibilité :** format exploitable (CSV, JSON structuré) — un log illisible est inutilisable en justice
- **Séparation des droits :** l'administrateur système ne doit pas pouvoir supprimer ses propres traces (logs vers serveur tiers ou solution SIEM externe)

> *⚠ Un log modifiable ou dont l'horodatage est non synchronisé ne peut pas constituer une preuve. Ces deux points sont les premières questions soulevées en cas de contentieux.*

2. Événements Redoutés et Scénarios de Risque

2.1 Vocabulaire clé

Terme	Définition
Événement redouté	Situation crainte : perte de confidentialité, d'intégrité ou de disponibilité d'un bien
Bien support	Ce qui est menacé : BDD, application, fichier, réseau, compte utilisateur
Source de menace	Qui pourrait provoquer l'événement redouté ? (acteur)
Scénario de risque	Enchaînement cause → vecteur d'attaque → événement redouté
Abuser story	Reformulation d'une user story du point de vue d'un attaquant
Mesure de sécurité	Contrôle technique ou organisationnel réduisant la probabilité ou l'impact

2.2 Structure d'un tableau d'impacts

Pour chaque événement redouté, l'examinateur attend : l'impact métier/technique, et la gravité (issue de la matrice P×I).

N°	Événement redouté	Bien support	Impacts pour l'entreprise	Gravité
1	Vol des données clients (nom, email, paiement)	BDD clients, API REST	Violation RGPD → notification CNIL, amendes jusqu'à 4% CA, perte de confiance clients, contentieux, atteinte à la réputation	Critique (P=3, I=4)
2	Indisponibilité de l'application en période de pointe	Serveur web, infra cloud	Perte de chiffre d'affaires, pénalités contractuelles SLA, frustration clients, désavantage concurrentiel	Élevée (P=3, I=3)
3	Altération des billets PDF générés	Module de génération PDF, stockage fichiers	Fraude possible (faux billets valides), engagements contractuels non respectés, perte de revenus, atteinte à l'intégrité du système billettique	Élevée (P=2, I=4)
4	Impression non autorisée de billets PDF	Fonction d'impression, contrôle d'accès	Distribution frauduleuse de billets, pertes financières, impossibilité de contrôler les entrées, atteinte à l'équité entre utilisateurs	Élevée (P=3, I=3)

2.3 Mesures lors du développement

L'événement redouté 4 porte sur l'impression frauduleuse de billets PDF. Les mesures sont à intégrer dès le sprint de développement :

Catégorie	Mesure à implémenter	Justification
Contrôle d'accès	Vérification serveur de l'authentification avant génération du PDF - jamais côté client seul	Empêche la génération sans compte valide authentifié
Unicité du billet	Identifiant unique non-prédictible (UUID v4) encodé dans le PDF + QRcode signé cryptographiquement	Rend la duplication ou falsification détectable au contrôle
Limitation d'impression	Compteur côté serveur : chaque billet ne peut être généré/imprimé qu'une fois (flag is_printed en BDD)	Bloque la réimpression multiple d'un même billet valide
Signature numérique du PDF	Le serveur signe le PDF avec une clé privée (PKI interne) - vérifiable par le système de contrôle à l'entrée	Garantit l'authenticité et l'intégrité du document
Journalisation	Log horodaté de chaque génération (user_id, ticket_id, timestamp, IP)	Traçabilité en cas de contestation ou fraude détectée
Rate limiting	Limiter le nombre de générations PDF par compte et par heure	Prévient les abus automatisés (scripts de génération en masse)

2.4 Scénario de risque complet — Abuser story (A2.3)

▸ Événement redouté 3 : Altération des billets PDF

Abuser story (scénario de risque) :
« En tant qu'attaquant ayant obtenu un accès au stockage des fichiers PDF (via une vulnérabilité de traversée de répertoire ou des droits trop permissifs sur le serveur), je veux modifier le contenu d'un fichier billet.pdf afin de remplacer l'identifiant ou la date de validité par des valeurs frauduleuses, permettant l'entrée illégale à un événement ou la revente de billets falsifiés. »

Enchaînement du scénario :

- Reconnaissance : l'attaquant identifie que les PDF sont stockés dans /uploads/billets/ accessible via l'URL directe
- Vecteur d'accès : exploitation d'une faille de path traversal (../../../) ou d'un bucket S3 mal configuré (public en écriture)
  - Action malveillante : modification du QRcode ou du texte visible du billet (nom, date, siège)
  - Impact : des billets falsifiés circulent — contrôle à l'entrée compromis

Mesure à prévoir	Type	Effet
Stocker les PDF hors du webroot (dossier non accessible directement via URL)	Technique	Supprime l'accès direct aux fichiers
Servir les PDF via un endpoint authentifié (GET /billet/{uuid} avec vérification de session)	Technique	Contrôle d'accès à chaque téléchargement
Signature numérique du PDF (hash SHA-256 + clé privée) stocké en BDD	Technique	Toute modification invalide la signature
Permissions système restrictives sur le dossier de stockage (lecture seule pour l'applicatif)	Technique	Empêche l'écriture même en cas d'accès
Vérification de l'intégrité du PDF à chaque consultation (hash recalculé vs BDD)	Technique	Détection immédiate de toute altération
Audit log de tous les accès aux fichiers PDF	Organisationnelle	Traçabilité pour investigation post-incident

2.5 Proposer des événements redoutés à partir d'une user story

▸ Méthode : du récit utilisateur aux événements redoutés

Pour identifier les événements redoutés d'une user story, appliquer cette démarche systématique :

- **1. Lister les données manipulées :** quelles informations circulent ? (Données personnelles, financières, fichiers…)
- **2. Identifier les actions critiques :** connexion, paiement, téléchargement, modification…
- **3. Appliquer la triade DIC :** que se passe-t-il si la donnée est divulguée ? altérée ? inaccessible ?
- **4. Formuler l'événement :** « Perte de [critère] de [bien support] par [source de menace] »

Exemple: « En tant qu'acheteur, je veux payer ma commande par carte bancaire »

Événement redouté	Critère DICT	Source de menace	Gravité estimée
Interception des données bancaires (numéro de carte, CVV) lors de la transmission	Confidentialité	Cybercriminel externe (attaque MitM, écoute réseau)	Critique - impact financier direct sur l'acheteur, responsabilité légale DSP2/PCI-DSS
Altération du montant de la transaction avant traitement par la banque	Intégrité	Attaquant interne ou externe ayant accès à la couche applicative	Critique - fraude financière, perte directe, litiges
Indisponibilité du module de paiement en période de forte charge	Disponibilité	Défaillance technique (sûreté) ou DDoS ciblé (sécurité)	Élevée - perte de CA, abandon de panier, SLA
Absence de trace horodatée en cas de contestation de paiement par l'acheteur	Traçabilité	Employé négligent (logs désactivés) ou défaillance de la solution de paiement	Élevée - contentieux non défendable, remboursement forcé

> 💡 *En épreuve : proposer systématiquement au moins un événement par critère DICT. Cela démontre une lecture structurée de la user story et une maîtrise de la méthode.*