

Descriptif de module 65-43

Domaine : Economie & Services
Filière : Informatique de gestion

1. Intitulé de module	Analyse d'impact	2026-2027
Code : 65-43 Niveau : ☐ Module de base ☐ Module d'approfondissement ☐ Module avancé ☐ Module spécialisé ☒ Autres : Option Type : ☐ Module principal ☐ Module lié au module principal ☐ Module facultatif ou complémentaire ☒ Autres : Option	Type de formation : ☒ Bachelor ☐ Master ☐ MAS ☐ DAS ☐ CAS ☐ Autres : Caractéristique : ☒ Module dont l'échec peut entraîner l'exclusion définitive de la filière selon l'art. 32, al. 1 du Règlement sur la formation de base en HES-SO. Organisation temporelle : ☐ Module sur 1 semestre ☐ Module sur 2 semestres ☒ Semestre d'automne ☐ Semestre de printemps ☐ Autres :	

2. Organisation

Crédits ECTS

5

Langue principale d'enseignement :

- | | |
|--|----------------------------------|
| ☒ Français | ☐ Italien |
| ☐ Allemand | ☐ Anglais |
| ☐ Autres : | |

3. Prérequis

- ☐ Avoir validé le module
☒ Avoir suivi les modules 63-22 et 61-31
☐ Pas de prérequis
☐ Autres :

4. Compétences visées / Objectifs généraux d'apprentissage

L'AIPD est abordée comme une méthode professionnelle d'analyse et de décision permettant de croiser protection des données, architecture technique, cybersécurité et besoins métier.

À la fin du module, l'étudiant-e sera capable de :

- Analyser un traitement de données en articulant exigences juridiques, architecture technique, menaces, vulnérabilités et mesures de cybersécurité
- Réaliser et documenter une analyse d'impact relative à la protection des données (AIPD) dans un contexte professionnel suisse
- Identifier et évaluer les risques juridiques et techniques liés à un traitement de données, ainsi que leurs conséquences pour les personnes concernées
- Proposer et justifier des mesures juridiques, organisationnelles et techniques adaptées aux risques identifiés
- Évaluer l'efficacité des mesures mises en œuvre et le risque résiduel
- intégrer les enjeux de durabilité numérique dans les choix de traitement et d'architecture, notamment par la minimisation des données, la maîtrise des durées de conservation et la sobriété des ressources
- Formuler et défendre une recommandation argumentée quant à la mise en œuvre d'un traitement

5. Objectifs détaillés des enseignements

Objectifs principaux :

À l'issue du module, l'étudiant-e sera en mesure de :

- Cartographier les acteurs, les données, les systèmes et les flux d'un traitement
- Identifier les exigences juridiques applicables, notamment en matière de finalité, proportionnalité, minimisation, transparence, durée de conservation et protection des données dès la conception et par défaut
- Identifier les enjeux particuliers liés aux données sensibles, au profilage, aux décisions automatisées, à la sous-traitance et aux transferts de données
- Identifier les actifs, menaces, vulnérabilités, surfaces d'attaque et scénarios de risque liés au traitement
- Mobiliser des méthodes et référentiels d'analyse des risques et de sécurité, notamment ISO 27005 et EBIOS RM
- Évaluer les risques selon leur gravité et leur vraisemblance
- Concevoir des mesures juridiques, organisationnelles, humaines et techniques permettant de réduire les risques
- Apprécier la robustesse et l'efficacité des contrôles de sécurité mis en œuvre
- Réagir à un incident de sécurité et réévaluer l'AIPD lorsque le traitement ou son contexte évolue
- Arbitrer entre exigences de protection des données, sécurité, performance et durabilité numérique
- Documenter, hiérarchiser et communiquer les résultats de l'analyse afin de soutenir une décision professionnelle

6. Plan et chapitres des cours

- Introduction à l'AIPD et identification des traitements à risque élevé
- Cartographie du traitement : acteurs, données, systèmes, flux et architecture
- Principes de protection des données et conception du traitement
- Analyse juridique et technique des traitements à risque, notamment IA, profilage, cloud, API, sous-traitance et transferts
- Analyse des risques : scénarios, menaces, vulnérabilités, gravité et vraisemblance
- Mesures de sécurité et traitement des risques : mesures juridiques, organisationnelles et techniques
- Gestion d'incident, risque résiduel, documentation et décision finale

7. Forme et méthodes pédagogiques**Utilisation de l'IA dans le cadre du module**

Dans le cadre du cours : L'usage de l'IA est déconseillé, sauf dans les cas et selon les modalités spécifiées dans le cadre du cours. Toute utilisation de l'IA doit faire l'objet d'une mention pertinente et transparente.

Dans le cadre des évaluations : Aucune utilisation

Le module combine, à poids équivalent, des apports juridiques et des apports techniques en cybersécurité.

Un cas fil rouge évolutif accompagne l'ensemble du module. Les étudiant-es travaillent en équipes et analysent progressivement un projet numérique dont la complexité augmente au fil des séances.

Les activités comprennent des apports théoriques, des cartographies de traitements et de flux, des analyses de scénarios de risque, l'utilisation de méthodes et référentiels professionnels, la conception de mesures de réduction des risques, des mises en situation et simulations, ainsi que la réalisation progressive d'une AIPD complète.

Des outils interactifs sont utilisés pour favoriser la participation, le questionnement et la confrontation des analyses.

Le module se conclut par la présentation et la défense des conclusions de l'AIPD devant un comité de décision simulé.

Utilisation de l'IA dans le cadre du module

Dans le cadre du cours : L'usage de l'IA est déconseillé, sauf dans les cas et selon les modalités spécifiées dans le cadre du cours. Toute utilisation de l'IA doit faire l'objet d'une mention pertinente et transparente.

Dans le cadre des évaluations : Aucune utilisation

8. Modalités d'évaluation et de validation

Présence :

La présence à toutes les activités d'enseignement est obligatoire et constitue une condition de validation du module. Tout absence doit être justifiée au près du secrétariat dans les 48 heures suivant l'absence.

Les étudiant-e-s dont le taux de présence est inférieur à 90% ne sont pas autorisé-e-s à réaliser l'évaluation finale ce qui entraîne la note de 1 pouvant entraîner l'échec au module.

L'évaluation du module se fera en principe de la manière suivante :

L'évaluation du cours est répartie entre un travail individuel et un travail en groupe.

Évaluation individuelle (50 %)

Contrôle continu comprenant : cas pratiques, QCM et questions ouvertes

Évaluation en groupe (50 %)

Rendus intermédiaires (20 %)

Évaluation basée sur : le suivi du projet, la qualité du contenu et la pertinence des analyses

Rapport final (80 %)

Qualité du rapport écrit 30 %

Présentation orale et questions 70 %

Acquis : A-E

Remédiation : Fx

Répétition : F

Remédiation / Fx :

Un module pour lequel l'étudiant-e obtiendrait une note entre 3.5 et 3.9 peut faire l'objet d'une remédiation, conformément à l'art. 29 al. 1 du Règlement sur la Formation de base en HES-SO.

Si la remédiation est validée la note de 4 sera attribuée.

Si la remédiation n'est pas validée le module sera répété.

Répétition / F :

Un module pour lequel l'étudiant-e obtiendrait une note inférieure ou égale à 3.4 doit être répété.

L'étudiant-e qui n'obtient pas les crédits attribués à un module doit le répéter dès que possible, conformément à l'art. 30 al. 1 du Règlement sur la formation de base en HES-SO.