Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle CYB1103 Gr. 01
Titre : Gouvernance en cybersécurité et gestion de risque
Session : Hiver 2025 **Horaire et local**
Professeur : Said, Dhaou

1. Description du cours paraissant à l'annuaire :

Objectifs
Au terme de ce cours, l'étudiant.e sera initié.e aux moyens de gestion de la sécurité informationnelle ainsi qu'aux moyens de régulation des systèmes de sécurité mis en place dans une entreprise pour atteindre ses objectifs.

Contenu

La cybersécurité en tant que décision d'affaire. Principes de gouvernance appliqués aux technologies de l'information des entreprises. Survol des TI et de la sécurité en entreprise. Aperçu des référentiels de gouvernance des TI (COBIT et ISO 38500). Alignement stratégique des TI aux affaires. Gestion des risques TI. Cadres de contrôle. Cadre réglementaire (Conformité). Cadre normatif. Fonctions de surveillance. Pratique d'audit interne. Survol de plateformes de gestion de la gouvernance des risques et de la conformité (GRC). Enjeux et défis rencontrés en gouvernance des TI et de la sécurité en entreprise. Résolution de problèmes de gouvernance et de gestion de risque tirés du monde réel. Ce cours comporte des séances **obligatoires** de travaux pratiques (TP).

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

- Comprendre les enjeux stratégiques de la gouvernance, des risques et de la conformité (GRC)
- Connaître les principaux cadres normatifs et cadres de gestion utilisés en GRC au Canada
- Être en mesure de réaliser des analyses de risque TI
- Être en mesure de faire des recommandations aux entreprises, organisations et leurs gestionnaires en GRC.

3. Stratégies pédagogiques :

Les formules pédagogiques suivantes seront utilisées :

C'est un cours NON PRESENTIEL

Logistique du cours
Plan synthétisé du cours
Les thèmes suivants seront étudiés :

1. Introduction à la Gouvernance en Cybersécurité
   - Définition et objectifs de la gouvernance en cybersécurité
   - Modèles de gouvernance en cybersécurité
   - Réglementations et normes de cybersécurité
2. Cadres et Modèles de Gestion des Risques en Cybersécurité
   - Principes de la gestion des risques en cybersécurité
   - Modèles et cadres de gestion des risques
   - Outils de gestion des risques
3. Identification et Évaluation des Risques
   - Processus d'identification des risques
   - Évaluation des risques
   - Gestion des risques émergents
   - Étude de cas réel (Target Corporation)
4. Contrôles et Stratégies de Mitigation des Risques
   - Contrôles de sécurité : Prévention, détection, réponse
   - Stratégies de mitigation des risques
   - Gestion des vulnérabilités

5. Gouvernance des Technologies de l'Information et de la Cybersécurité
   - Rôle du comité de gouvernance et des parties prenantes
   - Planification stratégique en cybersécurité
   - Reporting et communication en cybersécurité
   - Étude de cas réel (TESLA)
6. Culture de la Sécurité et Sensibilisation
   - Culture organisationnelle et cybersécurité
   - Gestion des comportements à risque
7. Gestion des Incidents et Réponse aux Crises
   - Réponse aux incidents de cybersécurité
   - Gestion de crise et communication
   - Analyse post-incident
8. Étude de Cas de Gouvernance en Cybersécurité et Gestion des Risques
   - Meta,
   - Hydro Quebec,
   - Amazon,
   - INRS,
   - Etc.

NOTE : *Toutes les parties du cours seront illustrées à l'aide des implémentations sur Python/Matlab pour la sécurité des systèmes informatisés : détection de vulnérabilités, détection d'intrusions, classification de malwares, identification et analyse de risques.*

4. Heures de disponibilité ou modalités pour rendez-vous :

Disponible avant les cours et sur rendez-vous.

Courriel : dhaou.said@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction à la Gouvernance en Cybersécurité : • Définition et objectifs de la gouvernance en cybersécurité • Modèles de gouvernance en cybersécurité, • Réglementations et normes de cybersécurité	15 jan. 2025
2	Cadres et Modèles de Gestion des Risques en Cybersécurité • Principes de la gestion des risques en cybersécurité • Modèles et cadres de gestion des risques • Outils de gestion des risques (Cartographie des risques, matrices de risque Outils logiciels pour la gestion des risques : RSA Archer, RiskWatch)	22 jan. 2025
3	Identification et Évaluation des Risques • Processus d'identification des risques • Évaluation des risques • Gestion des risques émergents **Travaux dirigés 1 : Étude de cas réel (Target Corporation)**	29 jan. 2025
4	Contrôles et Stratégies de Mitigation des Risques : • Contrôles de sécurité : Prévention, détection, réponse • Stratégies de mitigation des risques • Gestion des vulnérabilités	5 fév. 2025
5	Gouvernance des Technologies de l'Information et de la Cybersécurité • Rôle du comité de gouvernance et des parties prenantes • Planification stratégique en cybersécurité • Reporting et communication en cybersécurité **Travaux dirigés 2** : **Étude de cas réel (TESLA)**	12 fév. 2025

6	**Semaine d'études** Culture de la Sécurité et Sensibilisation • Culture organisationnelle et cybersécurité • Gestion des comportements à risque **Travaux dirigés 3** : **Étude de cas réel (E-Shop-Inc.)**	19 fév. 2025
7	Gestion des Incidents et Réponse aux Crises • Réponse aux incidents de cybersécurité • Gestion de crise et communication • Analyse post-incident	26 fév. 2025
8	**Semaine d'études**	3 au 7 mars 2025
9	**Examen de mi-session** – **En non présentiel.** Pondération : 30 %	12 mars. 2025
10	**Travaux dirigés 4** : Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Meta (anciennement Facebook)	19 mars. 2025
11	**Travaux dirigés 5** :Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez INRS Québec (**Ransomware attack** 2022)	26 mars. 2025
12	**Travaux dirigés 6** Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Amazon	02 avril 2025
13	**Travaux dirigés 7 :** Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Hydro Quebec	9 avril 2025
14	Conclusion et récapitulatif • Synthèse des concepts clés ○ Résumé des principaux enseignements en gouvernance et gestion des risques ○ Préparation à l'évaluation finale • Préparation à la mise en œuvre ○ Comment appliquer les connaissances acquises dans des projets réels ○ Outils et ressources pour la gestion continue de la cybersécurité et des risques • Évaluation et examen final ○ Études de cas pratiques et analyse de scénarios de gouvernance et de gestion des risques ○ Examen théorique et pratique sur la gestion des risques et la gouvernance en cybersécurité	16 avril 2025
15	**Examen final – En non présentiel – Pondération : 40%**	23 avril 2025

6. Évaluation du cours :

L'étudiant(e) dans ce cours sera évalué(e) par les examens de mi-session et final, ainsi que par des travaux pratiques. La pondération de la note finale sera comme suit :

- Examen de mi-session : **30 %**
- Examen final : **40 %**
- Travaux pratiques : **30 %**

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO

- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.
Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

[1] RGPD (Règlement général sur la protection des données).
[2] Loi californienne sur la protection de la vie privée des consommateurs (CCPA)
[3] Loi sur les services numériques (DSA) et sur le marché numérique (DMA) en Europe et en États Unies.
[4] https://ised-isde.canada.ca/ site/isde/fr/reglement-general-protection-donnees-rgpd
[5] https://gdpr-info.eu

9. Page Web du cours :

https://moodle.uqo.ca