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 2026 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 :

À la fin de ce cours l'étudiant sera capable de :

1. Établir une politique de cybersécurité robuste
   - Développer une politique de cybersécurité alignée sur les objectifs stratégiques de l'organisation.
   - Définir clairement les rôles et responsabilités en matière de sécurité pour chaque acteur de l'organisation.
   - Mettre en place des protocoles de gestion des incidents et de réponse aux crises.
2. Évaluer et gérer les risques liés à la cybersécurité
   - Identifier et évaluer les risques potentiels associés aux systèmes d'information et aux données sensibles.
   - Analyser les menaces internes et externes et leur impact sur l'organisation.
   - Appliquer une méthodologie de gestion des risques (probabilité x impact) pour prioriser les actions correctives.
   - Évaluer régulièrement l'efficacité des mesures de réduction des risques.
3. Assurer la conformité aux régulations et normes en cybersécurité
   - Garantir le respect des lois, régulations, et normes en matière de protection des données (ex. RGPD, NIST, ISO 27001).
   - Mettre en place des processus de surveillance et d'audit pour s'assurer de la conformité continue.
   - Implémenter des pratiques de gestion des données personnelles (privacy by design).
4. Renforcer les contrôles techniques et opérationnels de sécurité
   - Déployer des outils de sécurité pour protéger l'infrastructure contre les menaces : pare-feu, antivirus, cryptage, etc.
   - Implémenter des contrôles d'accès stricts (authentification multi-facteurs, gestion des droits d'accès).
   - Mettre en place des mécanismes de détection et de prévention des intrusions.
5. Mettre en place un cadre de gestion des incidents de cybersécurité
   - Développer un plan de gestion des incidents de cybersécurité incluant des procédures détaillées pour la détection, l'analyse, la réponse, et la récupération.
   - Former le personnel aux bonnes pratiques en matière de sécurité et à la gestion des incidents.
   - Tester régulièrement les plans de réponse aux incidents par le biais de simulations d'attaque (ex. : tests de pénétration, simulations de ransomware).

6. Garantir la continuité des activités en cas d'incident
   - Élaborer et mettre à jour des plans de continuité des activités (PCA) et de reprise après sinistre (DRP).
   - Assurer des sauvegardes régulières et déconnectées des systèmes critiques.
   - Tester les procédures de reprise pour minimiser le temps d'indisponibilité des services essentiels.

7. Promouvoir une culture de cybersécurité au sein de l'organisation
   - Sensibiliser et former l'ensemble des collaborateurs aux risques cyber et aux bonnes pratiques de sécurité.
   - Organiser des campagnes de sensibilisation régulières sur les menaces courantes (phishing, ransomwares, etc.).
   - Encourager une communication ouverte concernant les incidents de sécurité et la gestion des risques.

8. Effectuer une gestion proactive de la sécurité des données
   - Implémenter des stratégies de protection des données sensibles (cryptage, anonymisation, masquage).
   - Assurer la sécurité des données en transit et au repos.
   - Mettre en place une gestion des droits d'accès et de la confidentialité des données.

9. Assurer la surveillance et l'audit continu de la sécurité
   - Déployer des outils de surveillance en temps réel (SIEM) pour détecter les anomalies et les intrusions.
   - Réaliser des audits réguliers de la sécurité des systèmes et des infrastructures.
   - Mettre en place des mécanismes de reporting pour suivre l'état de la cybersécurité et des risques.

10. Mettre en place des stratégies de réduction de l'impact des cyberattaques
    - Développer des stratégies pour minimiser l'impact d'une attaque sur les opérations et la réputation de l'organisation.
    - Utiliser des solutions de sauvegarde et de restauration pour récupérer les données affectées.
    - Mettre en œuvre des actions pour limiter la propagation des attaques (ex. : isolation des systèmes compromis).

11. Améliorer la gestion des relations avec les parties externes
    - Évaluer les risques liés aux partenaires, fournisseurs, et autres tiers ayant accès aux systèmes.
    - Assurer la sécurité des échanges de données avec des parties externes (partenaires, clients, fournisseurs).
    - Mettre en place des accords de niveau de service (SLA) et des clauses de sécurité contractuelles avec les fournisseurs.

12. Anticiper les évolutions technologiques et les nouvelles menaces
    - Surveiller l'évolution des technologies et des tendances en matière de cybersécurité.
    - Adapter les pratiques de gestion des risques aux nouvelles menaces émergentes, telles que les ransomwares avancés, l'IA, ou les attaques par IoT.
    - Participer à des initiatives collaboratives et des forums pour partager des informations sur les menaces et les bonnes pratiques.

3. Stratégies pédagogiques :

Les formules pédagogiques suivantes seront utilisées :

Logistique du cours

- **Exposés magistraux** : présentation des concepts fondamentaux, cadres de gouvernance, normes et meilleures pratiques en cybersécurité et en gestion des risques.
- **Études de cas** : analyse de situations réelles ou simulées permettant d'illustrer les enjeux de gouvernance, de conformité et de gestion des risques cybernétiques.
- **Travaux pratiques et discussions dirigées** : échanges encadrés visant à développer l'esprit critique, la réflexion stratégique et la capacité d'argumentation.
- **Lectures ciblées** : articles scientifiques, normes (ISO, NIST, etc.) et documents professionnels pour approfondir les thématiques abordées.
- **Présentations étudiantes** : exposés individuels ou en équipe sur des sujets liés à la gouvernance, à la conformité réglementaire et à la gestion des risques en cybersécurité.

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	14 jan. 2026

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)	21 jan. 2026
3	Identification et Évaluation des Risques • Processus d'identification des risques • Évaluation des risques • Gestion des risques émergents **Travaux pratiques 1 : Étude de cas réel (Target Corporation) – ven. 29 jan. 2026**	28 jan. 2026
4	Contrôles et Stratégies de Mitigation des Risques : • Contrôles de sécurité : Prévention, détection, réponse • Stratégies de mitigation des risques • Gestion des vulnérabilités	4 fév. 2026
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 pratiques 2** : **Étude de cas réel (TESLA) – ven. 12 fév. 2026**	11 fév. 2026
6	Culture de la Sécurité et Sensibilisation • Culture organisationnelle et cybersécurité • Gestion des comportements à risque **Travaux pratiques 3** : **Étude de cas réel (E-Shop-Inc.) – ven. 19 fév. 2026**	18 fév. 2026
7	Gestion des Incidents et Réponse aux Crises • Réponse aux incidents de cybersécurité • Gestion de crise et communication • Analyse post-incident	25 fév. 2026
8	**Semaine d'études**	2-6 mars 2026
9	**Examen de mi-session** – **En non présentiel. Pondération : 30 %**	11 mars 2026
10	**Travaux pratiques 4** : Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Meta (anciennement Facebook)	18 mars 2026
11	**Travaux pratiques 5** : Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez INRS Québec (Ransomware attack 2022)	25 mars 2026
12	**Travaux pratiques 6 :** Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Amazon	01 avril 2026
13	**Travaux pratiques 7 :** Étude de Cas : Gouvernance en Cybersécurité et Gestion des Risques chez Hydro Québec	08 avril 2026
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	15 avril 2026

	○ Examen théorique et pratique sur la gestion des risques et la gouvernance en cybersécurité	
15	**Examen final – non présentiel – Pondération : 40%**	22 avril 2026

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