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

Sigle : CYB1053 Gr. 01
Titre : Audit en cybersécurité et conformité
Session : Hiver 2025 Horaire et local
Professeur : Caissy, David

1. Description du cours paraissant à l'annuaire :

Objectifs
Au terme de ce cours, l'étudiant.e sera en mesure d'appliquer les méthodes d'audit en cybersécurité à partir de cadres de référence et législatifs, d'évaluer le niveau de risque et de prioriser les actions pour combler les écarts de façon optimale.

Contenu

Notions de base de systèmes d'exploitation. Processus d'évaluation et autorisation de sécurité (EAS ou SA&A), obligations légales des organisations, standards et certifications en cybersécurité, analyse du contexte organisationnel et analyse de risque. Audit de plateformes Windows et Linux, de réseaux sans fils et de plateformes mobiles, et évaluation de la robustesse des configurations à l'aide de scripts PowerShell et SCCM. Mesures correctives et conditions minimales d'opération. Stratégies de communication et gestion de l'information. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

Descriptif - Annuaire

2. Objectifs spécifiques du cours :

Au terme de cette activité, l'étudiant, l'étudiante, doit démontrer une capacité à utiliser des outils et méthodes de gestion du risque rencontrant les normes reconnues et acceptées par l'industrie, en considérant du contexte particulier d'application des contrôles de sécurité pour rencontrer des besoins opérationnels spécifiques.

3. Stratégies pédagogiques :

Les stratégies pédagogiques suivantes seront utilisées, en **mode présentiel** :

- Cours magistraux
- Discussions de groupe
- Études de cas et travaux pratiques
- Examen de mi-session
- Examen final

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

Communication par courriel (david.caissy@uqo.ca) ou via Microsoft Teams. Période de consultation flexible sur rendez-vous.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	**Introduction** • L'importance de l'assurance de la conformité • Concepts de base de la sécurité de l'information • Conditions minimales d'opération	14 janv. 2025
2	**Classification de l'information** • Catégorisation des biens et du préjudice • Intégrité des données • Disponibilité des systèmes **Travail pratique 1 :** Classification de systèmes	21 janv. 2025

3	**Certification de la sécurité** • Exigences réglementaires de sécurité en fonction des données • Rôle de la certification pour l'assurance, l'audit et la conformité • Certification ISO-27000 • Norme PCI DSS pour les paiements par carte • Obligations légales des organisations **Travail pratique 2 :** Exigences de conformité requises	28 janv. 2025
4	**Audits de conformité** • Rôle du Centre canadien pour la cybersécurité • Mesures de protection du nuage du gouvernement du Canada • Présentation du processus SA&A • Les membres de l'équipe d'évaluation • Concept d'opérations	4 févr. 2025
5	**Protection de la vie privée** • Lois régissant la protection des données personnelles • Méthodologie spécifique aux informations sur la personne **Travail pratique 3 :** Évaluation de l'impact sur la vie privée	11 févr. 2025
6	**Processus de confirmation de la conformité** • Contrôles de sécurité ITSG-33 • Types de contrôles : techniques, opérationnels et administratifs • Familles de contrôles de sécurité	18 févr. 2025
7	**Examen de mi-session**	25 févr. 2025
8	**Semaine d'études**	4 mars 2025
9	**Collecte de preuves** • Documentation rigoureuse de la conformité • Présentation des preuves • Accès minimal requis **Travail pratique 4 :** Collecte de preuves	11 mars 2025
10	**Notions de base de systèmes d'exploitation** • Environnements traditionnels vs infonuagiques • Audit de plateformes Windows et Linux, de réseaux sans fils et de plateformes mobiles • Scripts PowerShell et SCCM	18 mars 2025
11	**Évaluation qualitative des vulnérabilités** • Méthodologie CVSS de qualification des vulnérabilités • Recherche de vulnérabilités et d'expositions courantes (CVE) • Évaluation de la menace **Travail pratique 5 :** Qualification des vulnérabilités	25 mars 2025
12	**Gestion du risque** • Corrélation entre biens, menaces et vulnérabilités • Probabilités et impacts • Mesures d'atténuation **Travail pratique 6 :** Gestion du risque	1er avril 2025
13	**Stratégies de communication et gestion de l'information** • Rapport d'évaluation de sécurité • Recommandations et mesures correctives • Plan d'action et jalons • Autorisation d'opérer	8 avril 2025

14	**La conformité de façon continuelle** • Intégrer l'audit aux changements • Assurer la conformité de façon continuelle • Évaluation de l'impact causé par des changements au système	15 avril 2025
15	**Examen final**	22 avril 2025

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes. Dans le cas spécifique du cours **Audit en cybersécurité et conformité**, l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 40 %**
- **6 travaux pratiques : 30 % (5% chacun)**
-

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 :

- Mesures de protection du nuage du gouvernement du Canada (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32787)
- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) (https://www.cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie)
- Politique sur la sécurité du gouvernement, Conseil du Trésor (https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=16578)
- Loi sur la protection des renseignements personnels et les documents électroniques, Site Web de la législation (Justice) (https://laws-lois.justice.gc.ca/fra/lois/p-8.6/index.html)

9. Page Web du cours :

https://moodle.uqo.ca