PRATIQUES de l'Audit et du Contrôle des Systèmes d'Information

Janvier 2025

AUDIT
DES SYSTEMES D'INFORMATION

Exposés par binômes

Pratiques de l'Audit des Systèmes d'Information

MINKA Thierry

THEMES D'EXPOSE POUR LES ETUDIANTS

DE 3e ANNEE EN

AUDIT DES SYSTEMES D'INFORMATION

Table des matières

Répartition des étudiants par thème

Les thèmes présentés dans ce document sont conçus pour permettre à chaque étudiant, **individuellement**, de fixer les notions abordées en détail ou survolées en classe. A cet effet, ils vous sont donc répartis par binômes.

Tableau 1: Liste des binômes par thème d'exposé

NOMS	N° du Thème	NOMS	N° du Thème
☑ NGUEGANG LUCRESSE ☑ NANTIA AXEL	**1**	☑ MBETSI LINDSEY ☑ ONGUENE JESSICA	**2**
☑ CHEUTCHEU HILARY ☑ ZE MVONDO	**3**	☑ TAPA LOIC ☑ BIVEE CREOLD	**4**
☑ MENGUE BISSA ☑ NZOUCK TOUMPE	**5**	☑ FANTA YADON ☑ MEKOULOU GRAZIELLA	**6**
☑ TCHADJIE ANDERSON ☑ CHAHO JACKY	**7**	☑ NGUEMO AURELLE ☑ AFANE MANUELLA	**8**
☑ NDJEBAYI NATANAEL ☑ NGWAMBE MARIELLA	**9**	☑ DJOUKA JENNIFER ☑ ONOMO ALICE	**10**
☑ KALDAKAK ADAMA ☑ BAALAWE LIONEL	**12**	☑ KWEM PEK ☑ NGONDOUM NDENGUE	**11**
☑ WANSI GILDAS ☑ KOUGANG KEVINE	**14**	☑ GHOUMO OLIVIA ☑ DSAMAGO TRESOR	**15**
☑ MAKEU BELVA ☑ DJIELO DAVILA	**16**	☑ EMBOLO DOUGLAS ☑ MELONE VLADIMIR	**17**
☑ MADINAH AICHA ☑ JIANKAM SAMUEL	**18**	☑ OWONO MARTIN ☑ AYOMENE VARESE	**19**
☑ MVONGO FAREL ☑ TSAKENG CLAUDY	**20**	☑ FOUDA CASIMIR ☑ MINYANDA	**21**
☑ EKANI ESSABA ☑ DJOH CLAUDE	**23**	☑ HEYA SALOMON ☑ NNA FRANCIS	**22**
☑ BAGNY TEKAM ☑ ENAMASSEH ONGA	**24**	☑ ELOU'OU NDONG ☑ MBOUO IDA	**25**
☑ BASSEK JOSCA ☑ OBOUNOU ONDOA	**26**	☑ MAGUENA NDENE ☑ METO'O YAWA	**27**
☑ ENGOLO OBELE ☑ FORSI NJOYA	**28**	☑ ABDOURAHMANE ☑ DIFFO	**29**
☑ ATCHOUMENE JOYCE ☑ ATEUGONG TAKAN	**30**	☑ DJEUMENI TIOGANG ☑ DJOUMESSI IDA	**31**
☑ EYENGA ZIBI ☑ FOKOUO LUCIANO	**33**	☑ GUIADEM REVINE ☑ MEFO EVINA	**32**

☑ MOUAFFO SOKENG ☑ NINKOUONG PASCALE	**34**	☑ OYONO LYNN SHA ☑ TCHINDA TATISSONG	**35**
☑ TENE TAKOUNGA ☑ TONYE JOSEPH	**36**	☑ SAHA KOUCHELE ☑ NGO MOMHA	**37**

Source : Liste de la classe, Liste des exposés.

PS : Laissez le Délégué, **MON Délégué**, tranquille, c'est moi-même suivant un algorithme qui m'est propre, qui ai conçu les binômes.

Thème 1: Analyse et Évaluation de la Gouvernance des Systèmes d'Information selon COBIT 2019

1. Objectif d'apprentissage

L'objectif est d'amener l'étudiant à comprendre et appliquer un cadre méthodologique structuré pour l'évaluation de la gouvernance des SI en s'appuyant sur **COBIT 2019**. L'étudiant développera ainsi une approche critique et méthodique pour l'audit des SI en entreprise.

2. Objectifs pédagogiques

À l'issue de cet exposé, l'étudiant devra être capable de :

- ☑ Comprendre le cadre COBIT 2019 : Présenter les principes fondamentaux de COBIT, ses composantes et son rôle dans la gouvernance des SI.
- ☑ Identifier les domaines et processus clés : Expliquer la structuration de COBIT en domaines de gouvernance et en objectifs de gestion.
- ☑ Analyser la maturité des processus SI : Déterminer comment évaluer la maturité et la performance des processus SI selon COBIT 2019.
- ☑ Élaborer un plan d'audit basé sur COBIT : Construire une méthodologie d'évaluation de la gouvernance SI et définir les critères d'audit.
- ☑ Formuler des recommandations d'amélioration : Identifier les lacunes et proposer des recommandations alignées sur les meilleures pratiques.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.

☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

☑ Un rapport bien structuré et argumenté avec des références académiques et professionnelles (normes, standards, articles scientifiques).

☑ Une grille d'évaluation des processus SI basée sur COBIT pour illustrer la méthodologie d'audit.

☑ Des recommandations pertinentes et réalistes applicables en entreprise.

☑ Une présentation orale convaincante démontrant la compréhension du cadre COBIT et son application en audit des SI.

Thème 2 : Audit de la Sécurité des Systèmes d'Information selon ISO 27001

1. Objectif d'apprentissage

Comprendre les exigences de l'ISO 27001 et appliquer une méthodologie d'audit pour évaluer la conformité d'un Système d'Information aux principes de la norme.

2. Objectifs pédagogiques

- ☑ Comprendre la norme ISO 27001 et son application en audit des SI.
- ☑ Identifier les contrôles de sécurité requis et leur évaluation.
- ☑ Construire une grille d'audit pour évaluer la mise en conformité.
- ☑ Analyser un cas d'étude pour détecter les écarts et formuler des recommandations.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport structuré avec grille d'audit basée sur ISO 27001.
- ☑ Recommandations pour combler les non-conformités.
- ☑ Présentation synthétique avec analyse d'un cas réel ou fictif.

Thème 3 : Évaluation des Risques SI et Plan de Continuité d'Activité (PCA) selon ISO 22301

1. Objectif d'apprentissage

Acquérir une méthodologie d'évaluation des risques SI et concevoir un Plan de Continuité d'Activité (PCA) basé sur **ISO 22301**.

2. Objectifs pédagogiques

- ☑ Comprendre l'analyse des risques SI et la continuité d'activité.
- ☑ Appliquer la norme ISO 22301 à l'audit des PCA.
- ☑ Construire une matrice des risques et proposer un PCA réaliste.
- ☑ Analyser un scénario de cyberattaque ou panne critique et définir les mesures de mitigation.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Matrice des risques SI avec probabilité et impact.
- ☑ Plan de Continuité d'Activité détaillé.
- ☑ Présentation avec exemple de mise en œuvre en entreprise.

Thème 4 : Audit de la Gestion des Identités et des Accès (IAM) dans un SI

1. Objectif d'apprentissage

Évaluer l'efficacité des mécanismes de gestion des identités et des accès (IAM) et proposer des améliorations en matière de contrôle d'accès.

2. Objectifs pédagogiques

- ☑ Comprendre les principes de gestion des identités et des accès (IAM).
- ☑ Évaluer les risques liés aux droits d'accès excessifs.
- ☑ Construire une matrice d'audit des accès et tester l'application du principe de moindre privilège.
- ☑ Détecter des failles d'authentification et de gestion des rôles dans un SI donné.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport avec analyse des risques liés à IAM.
- ☑ Matrice des accès pour identifier les anomalies.
- ☑ Présentation des failles détectées et mesures d'atténuation.

Thème 5 : Détection et Analyse des Incidents de Sécurité dans un SI

1. Objectif d'apprentissage

Comprendre la gestion des incidents de sécurité et savoir utiliser des outils de détection et d'analyse des événements suspects.

2. Objectifs pédagogiques

- ☑ Apprendre les méthodologies de gestion des incidents en audit SI.
- ☑ Utiliser des outils de SIEM (Security Information and Event Management) pour analyser les logs.
- ☑ Identifier et classer les indicateurs de compromission (IoC).
- ☑ Simuler un scénario d'attaque et proposer un plan de réponse.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport avec étude d'un incident et analyse des logs.
- ☑ Présentation d'un plan de réponse structuré.
- ☑ Démonstration d'un outil SIEM ou forensic pour l'analyse d'incidents.

Thème 6 : Audit de la Sécurité des Applications Web et Vulnérabilités OWASP

1. Objectif d'apprentissage

Évaluer la sécurité des applications web à travers un audit basé sur les **10 principales vulnérabilités OWASP**.

2. Objectifs pédagogiques

- ☑ Comprendre les attaques les plus courantes sur les applications web.
- ☑ Tester des applications pour identifier les vulnérabilités OWASP.
- ☑ Appliquer une méthodologie d'audit de la sécurité applicative.
- ☑ Proposer des mesures correctives adaptées aux failles détectées.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillé avec analyse des vulnérabilités détectées.
- ☑ Démonstration d'un test d'intrusion sur une application web.
- ☑ Présentation des recommandations pour sécuriser l'application.

Thème 7 : Audit des Infrastructures Cloud et Conformité aux Bonnes Pratiques (ISO 27017 & ISO 27018)

1. Objectif d'apprentissage

Évaluer les risques liés à l'adoption du **Cloud Computing** et auditer la conformité aux normes de sécurité et protection des données dans un environnement Cloud.

2. Objectifs pédagogiques

- ☑ Comprendre les principes de sécurité du Cloud et les risques spécifiques.
- ☑ Appliquer ISO 27017 (sécurité du Cloud) et ISO 27018 (protection des données personnelles en Cloud).
- ☑ Construire une grille d'audit pour un environnement Cloud.
- ☑ Analyser un cas d'étude d'une migration Cloud et ses implications en audit SI.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Grille d'audit Cloud basée sur ISO 27017 & 27018.
- ☑ Étude de cas détaillant une évaluation de conformité Cloud.
- ☑ Présentation des failles potentielles et mesures correctives.

Thème 8 : Audit de la Gestion des Logs et Traçabilité dans un Système d'Information

1. Objectif d'apprentissage

Évaluer la gestion des **journaux d'événements (logs)** et leur rôle dans la traçabilité et la détection des incidents de sécurité.

2. Objectifs pédagogiques

- ☑ Comprendre l'importance de la gestion des logs dans l'audit SI.
- ☑ Identifier les meilleures pratiques de collecte, stockage et analyse des logs.
- ☑ Démontrer l'utilisation d'outils SIEM pour centraliser et analyser les logs.
- ☑ Simuler un scénario de détection d'un incident à partir des logs.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport avec analyse détaillée des logs d'un SI.
- ☑ Démonstration d'un outil SIEM appliqué à un cas réel ou fictif.
- ☑ Présentation des recommandations en gestion et conservation des logs.

Thème 9 : Audit de la Sécurité des Réseaux et Évaluation des Risques de Cyberattaques

1. Objectif d'apprentissage

Évaluer la posture de **sécurité d'un réseau informatique** et appliquer une méthodologie d'audit des risques cybernétiques.

2. Objectifs pédagogiques

- ☑ Comprendre les menaces et vulnérabilités des réseaux.
- ☑ Utiliser une méthodologie d'audit réseau (ISO 27001, NIST, CIS Controls).
- ☑ Tester la sécurité d'un réseau avec outils d'analyse (Nmap, Wireshark, etc.).
- ☑ Proposer un plan de renforcement de la cybersécurité réseau.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport incluant une analyse des vulnérabilités réseau.
- ☑ Démonstration de l'utilisation d'un outil de sécurité réseau.
- ☑ Présentation des recommandations pour sécuriser l'architecture réseau.

Thème 10 : Audit des Données et Évaluation de la Protection de la Vie Privée (GDPR & Lois sur la cybersécurité, la data protection, les communications électroniques, etc.)

1. Objectif d'apprentissage

Comprendre les **obligations légales et techniques** en matière de protection des données et évaluer la conformité d'une entreprise aux règlements comme le **GDPR**.

2. Objectifs pédagogiques

- ☑ Comprendre les principes de la protection des données et de la vie privée.
- ☑ Appliquer une méthodologie d'audit de conformité au GDPR et à la Loi Informatique et Libertés.
- ☑ Identifier les failles dans la gestion des données personnelles.
- ☑ Proposer un plan de mise en conformité pour une entreprise.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Grille d'audit de conformité GDPR.
- ☑ Analyse d'une fuite de données et plan d'amélioration.
- ☑ Présentation des actions correctives et bonnes pratiques.

Thème 11 : Évaluation des Risques liés à l'Intelligence Artificielle et Audit des Systèmes d'IA

1. Objectif d'apprentissage

Analyser les **risques liés à l'usage de l'IA** dans un Système d'Information et proposer une approche d'audit des **algorithmes et modèles d'IA**.

2. Objectifs pédagogiques

- ☑ Identifier les risques de sécurité et de biais dans les systèmes d'IA.
- ☑ Appliquer une méthodologie d'audit des algorithmes IA.
- ☑ Évaluer la conformité des modèles IA aux normes éthiques et réglementaires.
- ☑ Proposer des recommandations pour améliorer la transparence et la sécurité des modèles IA.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport avec une grille d'audit des modèles IA.
- ☑ Analyse d'un cas concret de dérive ou faille IA.
- ☑ Présentation des recommandations pour une IA responsable et sécurisée.

Thème 12 : Audit de la Sécurité des Objets Connectés (IoT) et Évaluation des Risques

1. Objectif d'apprentissage

Évaluer la sécurité des **objets connectés (IoT)** dans un SI et proposer une méthodologie d'audit pour identifier les vulnérabilités et réduire les risques liés aux dispositifs IoT.

2. Objectifs pédagogiques

- ☑ Comprendre les risques de sécurité des objets connectés (failles, attaques, gestion des mises à jour).
- ☑ Appliquer une méthodologie d'audit IoT basée sur les meilleures pratiques.
- ☑ Tester la sécurité d'un dispositif IoT à l'aide d'outils d'analyse.
- ☑ Proposer des recommandations pour sécuriser un environnement IoT.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport avec une grille d'audit IoT détaillant les risques et correctifs.
- ☑ Démonstration d'une analyse de vulnérabilités sur un objet connecté.
- ☑ Présentation des meilleures pratiques pour renforcer la sécurité IoT.

Thème 13 : Audit de la Sécurité des Bases de Données et Protection des Données Sensibles

1. Objectif d'apprentissage

Analyser la sécurité des **bases de données** et évaluer les mesures de protection des données sensibles contre les menaces internes et externes.

2. Objectifs pédagogiques

- ☑ Comprendre les principaux risques liés aux bases de données.
- ☑ Appliquer une méthodologie d'audit des bases de données.
- ☑ Identifier les attaques courantes (injection SQL, élévation de privilèges).
- ☑ Proposer des stratégies de sécurisation des bases de données.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant l'audit d'une base de données et ses vulnérabilités.
- ☑ Test d'injection SQL et démonstration d'une faille de sécurité.
- ☑ Présentation des recommandations pour améliorer la protection des bases de données.

Thème 14 : Audit de la Cybersécurité Industrielle et Sécurisation des SCADA

1. Objectif d'apprentissage

Évaluer les risques et sécuriser les **systèmes industriels (SCADA, ICS)** en appliquant des normes et bonnes pratiques en cybersécurité industrielle.

2. Objectifs pédagogiques

- ☑ Comprendre les spécificités et vulnérabilités des systèmes SCADA.
- ☑ Appliquer une méthodologie d'audit en cybersécurité industrielle.
- ☑ Identifier les attaques connues sur les systèmes industriels (ex. Stuxnet).
- ☑ Proposer des stratégies de protection des infrastructures critiques.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les vulnérabilités d'un système SCADA.
- ☑ Démonstration d'un scénario d'attaque simulé sur une infrastructure critique.
- ☑ Présentation des meilleures pratiques pour la sécurisation des systèmes industriels.

Thème 15 : Audit de la Sécurité des Services Web et API

1. Objectif d'apprentissage

Évaluer la sécurité des **services web et API** et appliquer des tests pour identifier les vulnérabilités les plus courantes.

2. Objectifs pédagogiques

- ☑ Comprendre les menaces liées aux API et aux services web.
- ☑ Appliquer une méthodologie d'audit des API (REST, SOAP).
- ☑ Tester la sécurité d'une API et identifier les failles courantes (OWASP API Top 10).
- ☑ Proposer des recommandations pour renforcer la sécurité des services web.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport présentant une méthodologie d'audit d'API et ses résultats.
- ☑ Démonstration d'un test d'intrusion sur une API vulnérable.
- ☑ Présentation des recommandations pour sécuriser une API.

Thème 16 : Évaluation de la Sécurité des Messageries et Protection Contre le Phishing

1. Objectif d'apprentissage

Analyser la sécurité des systèmes de **messagerie électronique** et évaluer les mécanismes de protection contre les **attaques de phishing**.

2. Objectifs pédagogiques

- ☑ Comprendre les attaques courantes sur les messageries (phishing, spam, malware, spoofing).
- ☑ Identifier les mécanismes de sécurité des services de messagerie (SPF, DKIM, DMARC).
- ☑ Tester la résistance d'une entreprise aux attaques par phishing.
- ☑ Proposer des stratégies pour améliorer la protection des emails.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les vulnérabilités d'un système de messagerie.
- ☑ Démonstration d'un test de phishing et analyse des réactions des utilisateurs.
- ☑ Présentation des mesures de protection renforcées contre le phishing.

Thème 17 : Audit de la Sécurité des Applications Mobiles et Évaluation des Risques

1. Objectif d'apprentissage

Évaluer la sécurité des **applications mobiles** et identifier les vulnérabilités courantes pour proposer des solutions d'amélioration.

2. Objectifs pédagogiques

- ☑ Comprendre les principales menaces et attaques sur les applications mobiles.
- ☑ Appliquer une méthodologie d'audit de sécurité mobile (Android et iOS).
- ☑ Identifier les failles courantes (OWASP Mobile Top 10).
- ☑ Tester une application mobile et proposer des recommandations.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport d'audit de sécurité mobile détaillant les risques et correctifs.
- ☑ Démonstration d'un test de sécurité sur une application mobile.
- ☑ Présentation des recommandations pour sécuriser une application mobile.

Thème 18 : Audit des Architectures Zero Trust et Implémentation en Entreprise

1. Objectif d'apprentissage

Analyser l'**approche Zero Trust** et son application en audit des SI pour renforcer la sécurité d'une infrastructure informatique.

2. Objectifs pédagogiques

- ☑ Comprendre le concept de Zero Trust et son impact sur la cybersécurité.
- ☑ Évaluer les différences entre une architecture traditionnelle et Zero Trust.
- ☑ Appliquer une méthodologie d'audit Zero Trust.
- ☑ Étudier un cas d'implémentation Zero Trust en entreprise.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport présentant une analyse des stratégies Zero Trust.
- ☑ Matrice des avantages et défis d'implémentation Zero Trust.
- ☑ Présentation des recommandations pour sécuriser un SI via Zero Trust.

Thème 19 : Audit des Algorithmes Cryptographiques et Sécurisation des Données Sensibles

1. Objectif d'apprentissage

Évaluer la sécurité des **algorithmes de chiffrement** et proposer des recommandations pour la protection des données sensibles.

2. Objectifs pédagogiques

- ☑ Comprendre les principaux algorithmes de chiffrement et leur sécurité.
- ☑ Identifier les attaques cryptographiques courantes.
- ☑ Évaluer la robustesse d'un chiffrement dans un SI.
- ☑ Proposer des solutions pour renforcer la protection des données.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport analysant la sécurité des algorithmes cryptographiques.
- ☑ Exemple d'attaque simulée sur un chiffrement faible.
- ☑ Présentation des recommandations pour améliorer la sécurité cryptographique.

Thème 20 : Audit de la Sécurité des Blockchains et Analyse des Risques

1. Objectif d'apprentissage

Évaluer la **sécurité des blockchains** et analyser les vulnérabilités associées aux contrats intelligents et aux transactions numériques.

2. Objectifs pédagogiques

- ☑ Comprendre le fonctionnement des blockchains publiques et privées.
- ☑ Identifier les vulnérabilités et risques des blockchains.
- ☑ Appliquer une méthodologie d'audit des smart contracts.
- ☑ Étudier un cas d'attaque sur une blockchain et en tirer des leçons.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport sur la sécurité d'une blockchain avec une étude de cas.
- ☑ Exemple d'audit d'un smart contract et détection de failles.
- ☑ Présentation des recommandations pour sécuriser les transactions blockchain.

Thème 21 : Audit de la Cyberrésilience et Plan de Reprise après Sinistre (PRA)

1. Objectif d'apprentissage

Analyser la capacité d'un **SI à résister aux cyberattaques** et à garantir la continuité des opérations en cas de crise.

2. Objectifs pédagogiques

- ☑ Comprendre le concept de cyberrésilience et continuité d'activité.
- ☑ Appliquer une méthodologie d'audit du Plan de Reprise après Sinistre (PRA).
- ☑ Identifier les failles dans les processus de sauvegarde et redondance.
- ☑ Tester un scénario de récupération après incident.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport d'audit du PRA d'une entreprise.
- ☑ Démonstration d'une simulation de cyberattaque et réaction du SI.
- ☑ Présentation des recommandations pour renforcer la cyberrésilience.

Thème 22 : Audit de la Cybersécurité des Véhicules Connectés et des Systèmes Embarqués

1. Objectif d'apprentissage

Analyser les risques liés aux **véhicules connectés et systèmes embarqués** et appliquer une méthodologie d'audit pour évaluer leur sécurité.

2. Objectifs pédagogiques

- ☑ Comprendre les menaces sur les véhicules connectés et systèmes embarqués.
- ☑ Identifier les vulnérabilités dans les communications et capteurs (CAN Bus, Bluetooth, GPS, etc.).
- ☑ Appliquer une méthodologie d'audit des systèmes embarqués.
- ☑ Proposer des recommandations pour sécuriser un véhicule connecté.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant un audit de véhicule connecté.
- ☑ Démonstration d'une vulnérabilité (ex. sniffing CAN Bus).
- ☑ Présentation des recommandations pour améliorer la sécurité des systèmes embarqués.

Thème 23 : Audit de la Sécurité des Réseaux 5G et Protection Contre les Attaques

1. Objectif d'apprentissage

Évaluer la sécurité des **réseaux 5G** et analyser les menaces spécifiques à cette technologie émergente.

2. Objectifs pédagogiques

- ☑ Comprendre l'architecture des réseaux 5G et ses risques.
- ☑ Identifier les vulnérabilités spécifiques aux infrastructures 5G.
- ☑ Appliquer une méthodologie d'audit des réseaux mobiles.
- ☑ Proposer des solutions pour sécuriser les communications 5G.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport analysant la cybersécurité des réseaux 5G.
- ☑ Identification des failles potentielles et solutions d'atténuation.
- ☑ Présentation des recommandations pour une 5G sécurisée.

Thème 24 : Audit de la Sécurité des Technologies de Reconnaissance Faciale et Biométriques

1. Objectif d'apprentissage

Évaluer la fiabilité et les risques liés aux **technologies biométriques** (reconnaissance faciale, empreintes digitales, etc.) et leur impact en cybersécurité.

2. Objectifs pédagogiques

- ☑ Comprendre les principes des technologies biométriques et leur usage.
- ☑ Identifier les failles et contournements possibles (deepfake, spoofing, etc.).
- ☑ Appliquer une méthodologie d'audit des solutions biométriques.
- ☑ Proposer des recommandations pour renforcer la sécurité de l'authentification biométrique.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les vulnérabilités des technologies biométriques.
- ☑ Test de contournement d'une solution biométrique.
- ☑ Présentation des recommandations pour une biométrie sécurisée.

Thème 25 : Audit des Deepfakes et Sécurité de l'Information Face à la Désinformation

1. Objectif d'apprentissage

Analyser l'impact des **deepfakes** en cybersécurité et proposer des stratégies pour détecter et atténuer les risques liés à la désinformation numérique.

2. Objectifs pédagogiques

- ☑ Comprendre les technologies derrière les deepfakes et leur évolution.
- ☑ Identifier les menaces en cybersécurité et manipulation de l'information.
- ☑ Appliquer une méthodologie d'audit des médias numériques.
- ☑ Étudier des outils de détection des deepfakes et leur efficacité.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant l'impact des deepfakes sur la cybersécurité.
- ☑ Test d'un outil de détection de deepfake.
- ☑ Présentation des recommandations pour lutter contre la désinformation.

Thème 26 : Audit de la Sécurité des Drones et des Systèmes de Communication Aérienne

1. Objectif d'apprentissage

Évaluer les risques liés aux **drones et systèmes de communication aérienne** et analyser les vulnérabilités en matière de cybersécurité.

2. Objectifs pédagogiques

- ☑ Comprendre les technologies utilisées dans les drones et leurs failles.
- ☑ Identifier les menaces de cybersécurité (piratage, brouillage, interception, etc.).
- ☑ Appliquer une méthodologie d'audit des systèmes embarqués des drones.
- ☑ Proposer des recommandations pour améliorer la sécurité des drones.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les vulnérabilités des drones et solutions d'atténuation.
- ☑ Démonstration d'une analyse de sécurité sur un drone.
- ☑ Présentation des recommandations pour renforcer la cybersécurité des drones.

Thème 27 : Audit des Systèmes d'Intelligence Artificielle et Évaluation des Risques Éthiques

1. Objectif d'apprentissage

Analyser la sécurité et les **risques éthiques des systèmes d'intelligence artificielle (IA)** et proposer des méthodes d'audit pour garantir leur fiabilité et leur transparence.

2. Objectifs pédagogiques

- ☑ Comprendre les principaux risques liés aux algorithmes d'IA (biais, manipulation, fiabilité).
- ☑ Identifier les vulnérabilités des modèles d'apprentissage automatique.
- ☑ Appliquer une méthodologie d'audit des systèmes d'IA.
- ☑ Étudier les cadres réglementaires et éthiques en matière d'IA (EU AI Act, IEEE, etc.).

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant une analyse des risques IA et solutions d'atténuation.
- ☑ Exemple de détection de biais ou d'attaque adversariale sur un modèle IA.
- ☑ Présentation des recommandations pour une IA sécurisée et éthique.

Thème 28 : Audit des Métavers et Sécurité des Identités Numériques

1. Objectif d'apprentissage

Évaluer les risques de cybersécurité dans les **métavers** et analyser les mécanismes de protection des **identités numériques**.

2. Objectifs pédagogiques

- ☑ Comprendre les enjeux de sécurité dans les métavers (falsification d'identité, vol de biens numériques, cyberharcèlement).
- ☑ Identifier les vulnérabilités des plateformes de réalité virtuelle et augmentée.
- ☑ Appliquer une méthodologie d'audit des infrastructures métavers.
- ☑ Proposer des recommandations pour sécuriser l'identité numérique et les transactions virtuelles.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les menaces du métavers et solutions de cybersécurité.
- ☑ Démonstration d'une faille ou d'une attaque sur un environnement virtuel.
- ☑ Présentation des recommandations pour sécuriser l'identité numérique dans le métavers.

Thème 29 : Audit de la Sécurité des Infrastructures Critiques et Protection Contre les Cyberattaques

1. Objectif d'apprentissage

Évaluer les risques et méthodologies d'audit pour **protéger les infrastructures critiques** (réseaux électriques, transports, hôpitaux, banques, etc.) contre les cyberattaques.

2. Objectifs pédagogiques

- ☑ Comprendre les menaces pesant sur les infrastructures critiques.
- ☑ Identifier les attaques connues (Stuxnet, NotPetya, Colonial Pipeline, etc.).
- ☑ Appliquer une méthodologie d'audit pour renforcer la sécurité.
- ☑ Proposer des solutions pour garantir la résilience et la protection des infrastructures critiques.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant l'évaluation de la sécurité des infrastructures critiques.
- ☑ Exemple d'audit d'un réseau industriel ou énergétique.
- ☑ Présentation des recommandations pour améliorer la cybersécurité des infrastructures critiques.

Thème 30 : Audit des Menaces Post-Quantiques et Sécurité des Systèmes Cryptographiques

1. Objectif d'apprentissage

Analyser les **menaces liées aux ordinateurs quantiques** et leur impact sur la cryptographie et la cybersécurité.

2. Objectifs pédagogiques

- ☑ Comprendre les principes des ordinateurs quantiques et leur menace sur les cryptosystèmes.
- ☑ Identifier les vulnérabilités des algorithmes de chiffrement classiques (RSA, ECC, AES).
- ☑ Appliquer une méthodologie d'audit de sécurité post-quantique.
- ☑ Proposer des solutions cryptographiques adaptées à l'ère quantique.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport analysant l'impact de l'informatique quantique sur la cybersécurité.
- ☑ Démonstration d'une simulation d'attaque quantique sur un algorithme classique.
- ☑ Présentation des recommandations pour adopter la cryptographie post-quantique.

Thème 31 : Audit de la Sécurité des Smart Cities et Gestion des Risques Urbains

1. Objectif d'apprentissage

Évaluer la **cybersécurité des infrastructures des villes intelligentes (Smart Cities)** et identifier les **vulnérabilités des systèmes connectés**.

2. Objectifs pédagogiques

- ☑ Comprendre les technologies des Smart Cities et leur intégration aux SI.
- ☑ Identifier les menaces et risques des infrastructures connectées.
- ☑ Appliquer une méthodologie d'audit des systèmes urbains intelligents.
- ☑ Proposer des recommandations pour renforcer la sécurité des Smart Cities.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les failles et solutions de cybersécurité pour les villes connectées.
- ☑ Exemple d'analyse d'un système de gestion urbaine intelligent.
- ☑ Présentation des recommandations pour une Smart City sécurisée.

Thème 32 : Audit de la Cybersécurité des Satellites et Systèmes Spatiaux

1. Objectif d'apprentissage

Analyser les **risques liés à la cybersécurité des satellites et infrastructures spatiales**, et proposer des méthodologies d'audit pour renforcer leur protection.

2. Objectifs pédagogiques

- ☑ Comprendre les technologies et protocoles de communication spatiale.
- ☑ Identifier les menaces sur les satellites et leurs systèmes embarqués (piratage, brouillage, interception).
- ☑ Appliquer une méthodologie d'audit des infrastructures spatiales.
- ☑ Proposer des solutions de sécurisation pour les communications et données satellitaires.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport analysant les vulnérabilités des satellites et infrastructures spatiales.
- ☑ Simulation d'un scénario de cyberattaque spatiale.
- ☑ Présentation des recommandations pour renforcer la cybersécurité des systèmes spatiaux.

Thème 33 : Audit des Risques liés aux Rançongiciels (Ransomware) et Stratégies de Protection

1. Objectif d'apprentissage

Évaluer les **menaces liées aux ransomwares**, analyser leur impact et proposer une méthodologie d'audit pour prévenir et répondre efficacement à ces attaques.

2. Objectifs pédagogiques

- ☑ Comprendre le fonctionnement des ransomwares et leur mode de propagation.
- ☑ Identifier les failles organisationnelles et techniques qui facilitent ces attaques.
- ☑ Appliquer une méthodologie d'audit et de prévention des ransomwares.
- ☑ Proposer des stratégies de remédiation et de réponse aux incidents.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant un audit des risques ransomware et solutions de protection.
- ☑ Simulation d'une attaque par ransomware et analyse des impacts.
- ☑ Présentation des recommandations pour une meilleure cyberrésilience.

Thème 34 : Audit des Cybermenaces dans le Domaine Médical et Sécurisation des Données de Santé

1. Objectif d'apprentissage

Analyser les **menaces et risques liés aux cyberattaques sur les infrastructures médicales** et proposer une méthodologie d'audit pour la protection des données de santé.

2. Objectifs pédagogiques

- ☑ Comprendre les enjeux de cybersécurité dans le domaine de la santé.
- ☑ Identifier les principales attaques contre les hôpitaux et systèmes médicaux.
- ☑ Appliquer une méthodologie d'audit des systèmes de santé (DMP, PACS, IoMT).
- ☑ Proposer des solutions pour protéger les infrastructures et données médicales.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les menaces et solutions de cybersécurité en santé.
- ☑ Démonstration d'une faille sur un système médical connecté.
- ☑ Présentation des recommandations pour sécuriser les données de santé.

Thème 35 : Audit des Menaces sur les Crypto-monnaies et Sécurisation des Transactions Blockchain

1. Objectif d'apprentissage

Analyser les **risques de cybersécurité liés aux crypto-monnaies** et évaluer les solutions de sécurisation des **transactions blockchain**.

2. Objectifs pédagogiques

- ☑ Comprendre le fonctionnement des crypto-monnaies et technologies blockchain.
- ☑ Identifier les attaques connues sur les plateformes d'échange et portefeuilles numériques.
- ☑ Appliquer une méthodologie d'audit des systèmes de gestion des crypto-actifs.
- ☑ Proposer des stratégies de protection pour sécuriser les transactions et portefeuilles.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les menaces sur les crypto-monnaies et solutions de protection.
- ☑ Simulation d'une attaque sur un portefeuille numérique.
- ☑ Présentation des recommandations pour sécuriser les actifs numériques.

Thème 36 : Audit de la Cybercriminalité Transnationale et Détection des Fraudes Numériques

1. Objectif d'apprentissage

Analyser les **techniques utilisées par les cybercriminels internationaux**, et proposer une méthodologie d'audit pour détecter et prévenir la fraude numérique.

2. Objectifs pédagogiques

- ☑ Comprendre les méthodes utilisées par les cybercriminels (fraude bancaire, phishing, dark web, etc.).
- ☑ Identifier les outils et techniques d'investigation numérique.
- ☑ Appliquer une méthodologie d'audit pour détecter les fraudes numériques.
- ☑ Proposer des solutions pour lutter contre la cybercriminalité transnationale.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les techniques des cybercriminels et solutions de prévention.
- ☑ Simulation d'un scénario de fraude numérique et analyse des indices.
- ☑ Présentation des recommandations pour renforcer la lutte contre la cybercriminalité.

Thème 37 : Audit de la Sécurité des Systèmes d'Intelligence Artificielle Générative et Détection des Abus

1. Objectif d'apprentissage

Analyser les **risques liés aux IA génératives** (ChatGPT, DALL-E, Midjourney, etc.), évaluer leur impact en cybersécurité et proposer des méthodes d'audit pour détecter et prévenir les abus.

2. Objectifs pédagogiques

- ☑ Comprendre les principes de fonctionnement des IA génératives et leur évolution.
- ☑ Identifier les menaces associées (deepfakes, usurpation d'identité, cyberattaques automatisées).
- ☑ Appliquer une méthodologie d'audit de la sécurité et de l'éthique des IA génératives.
- ☑ Proposer des solutions pour encadrer et sécuriser l'utilisation des IA génératives.

3. Instructions pour la production du rapport et de l'exposé

L'étudiant doit produire un **rapport structuré en cinq parties** et réaliser une **présentation orale** de 15 minutes.

3.1. Structure du rapport

- ☑ Introduction (1 à 2 pages)
- ☑ Présentation de la norme (3 à 4 pages)
- ☑ Audit de la conformité (4 à 6 pages)
- ☑ Recommandations et plan d'amélioration (2 à 3 pages)
- ☑ Conclusion et perspectives (1 à 2 pages)

3.2. Exigences de l'exposé oral

- ☑ Durée : 15 minutes (10 min de présentation + 5 min de questions).
- ☑ Support : Diaporama structuré (PowerPoint ou équivalent).
- ☑ Clarté et concision : Aller à l'essentiel avec des explications précises et des illustrations pertinentes.
- ☑ Interaction : Être capable de répondre aux questions et justifier ses choix méthodologiques.

4. Résultats attendus

- ☑ Rapport détaillant les menaces et solutions pour encadrer l'usage des IA génératives.
- ☑ Démonstration d'une détection d'abus (ex. fake news, deepfake, phishing automatisé).
- ☑ Présentation des recommandations pour une IA générative sécurisée et éthique.