CLUBEBIOS

Certification EBIOS Risk Manager

Exigences relatives aux compétences

Date	:	01/08/2020
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	9
Responsable des travaux	:	Club EBIOS
Validation	:	Groupe de travail
Approbation	:	Conseil d'administration
Licence	:	

Club EBIOS, 11 rue de Lourmel, 75015 PARIS

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
18/12/2012	Création du document sur la base des travaux du groupe des travaux du Club EBIOS relatifs à la certification de compétences EBIOS.	Matthieu GRALL	Document de travail
09/07/2017	Adaptation du document aux évolutions de contexte à l'aide des commentaires des administrateurs. Ajustement de l'introduction et redistribution du thème 4 Communication dans les 3 autres thèmes.	Matthieu GRALL Sonia AQUE François ZAMORA	Approuvé
01/08/2020	Améliorations multiples pour la cohérence avec EBIOS *Risk Manager* et les capacités attendues pour le niveau choisi.	Matthieu GRALL Jean OLIVE François ZAMORA	Approuvé

Sommaire

INTRODUCTION **4**

1 EXIGENCES RELATIVES À LA MAÎTRISE DES CONCEPTS **5**

Le risque en général 5
Le risque numérique en particulier 5
Les concepts dans la méthode 5
La gestion des risques numériques 5
La gestion des risques avec EBIOS *Risk Manager* 5

2 EXIGENCES RELATIVES À LA MAÎTRISE DE LA DÉMARCHE **6**

La démarche globale 6
Atelier 1 – Cadrage et socle de sécurité 6
Atelier 2 – Sources de risques 6
Atelier 3 – Scénarios stratégiques 6
Atelier 4 – Scénarios opérationnels 6
Atelier 5 – Traitement du risque 6

3 EXIGENCES RELATIVES À LA PRATIQUE DE LA MÉTHODE **7**

L'apprentissage de la méthode 7
La sensibilisation 7
L'organisation d'une étude 7
Les entretiens (recueil des informations) 7
Les réunions 7
Le choix du niveau de détail 7
La mise en œuvre d'études 7
L'obtention d'informations 7
Le travail en équipe 7
L'exploitation des bases de connaissances 7
L'obtention d'arbitrages 7
L'adaptation à la maturité de l'organisme 8
L'implication et la responsabilisation des acteurs 8
La production de livrables 8
L'obtention de validations 8
L'explication des conclusions 8

RÉFÉRENCES **9**

Introduction

Le présent document constitue le référentiel d'**[Exigences relatives aux compétences]** pour une certification de personnes portant sur leurs compétences relatives à la pratique de la méthode EBIOS *Risk Manager*[1].

Il définit les exigences de compétences exprimées par le Club EBIOS dans le cadre du schéma de certification de personnes pour la gestion des risques à l'aide de la méthode EBIOS *Risk Manager* (cf. **[Exigences relatives au schéma de certification])**

Il est organisé en trois **thèmes** complémentaires, de la théorie à la pratique :

1. Maîtrise des concepts
2. Maîtrise de la démarche
3. Pratique de la méthode

Ces thèmes sont déclinés en **critères** à évaluer, en **exigences**, représentant les capacités attendues par le niveau 2 du **[Référentiel de compétences]**.

À titre indicatif, des **exemples de points de contrôle** sont donnés à l'attention des organismes de certification.

[1] EBIOS *Risk Manager* est la méthode de gestion des risques numériques de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Critère	Exigences relatives aux compétences	Exemples de points de contrôle de l'évaluation du candidat
1 Exigences relatives à la maîtrise des concepts		
Le risque en général	1. Connaître et comprendre la définition du risque	✓ Il cite et explique une définition du risque compatible avec les normes internationales (ex : ISO 31000) ✓ Il explique les paramètres permettant de l'estimer
Le risque numérique en particulier	2. Connaître et comprendre la définition du risque numérique et de ses composantes	✓ Il donne une définition du risque proche de celle du glossaire de la méthode ✓ Il évoque tous les composants du risque (sources de risques, bien support, valeur métier, impacts) ✓ Il évoque les critères d'estimation des risques (gravité, vraisemblance) ✓ Il évoque et explique la notion de risques résiduels ✓ Il cite au moins un exemple de risque lié au contexte d'une étude de cas
Les concepts dans la méthode	3. Connaître et comprendre les concepts et la terminologie de la méthode	✓ Il donne une explication claire de deux des concepts de la méthode (valeur métier, bien support, socle de sécurité, événement redouté, source de risque, objectif visé, scénario stratégique, scénarios opérationnel, *etc*.) ✓ Il cite au moins un exemple lié au contexte spécifique d'une étude de cas
La gestion des risques numériques	4. Connaître et comprendre la définition normative de la gestion des risques et de ses sous-processus	✓ Il cite et décrit les sous-processus de gestion des risques, tels que définis dans la norme ISO/IEC 27005 ✓ Il décrit les principes de tenue à jour du plan de traitement des risques ✓ Il donne des exemples de facteurs (internes ou externes à l'organisme) qui peuvent engendrer une mise à jour de l'étude
La gestion des risques avec EBIOS *Risk Manager*	5. Comprendre en quoi la méthode contribue à la gestion des risques	✓ Il explique en quoi chaque atelier d'EBIOS *Risk Manager* contribue à chaque sous-processus de la gestion des risques numériques, tels que définis dans la norme ISO/IEC 27005

Critère	Exigences relatives aux compétences	Exemples de points de contrôle de l'évaluation du candidat
2 Exigences relatives à la maîtrise de la démarche		
La démarche globale	6. Comprendre les objectifs de la méthode 7. Comprendre les principaux enjeux de chaque atelier	✓ Il décrit les objectifs généraux de la méthode et les enjeux de chaque atelier ✓ Il donne au moins 3 exemples distincts du contexte d'utilisation d'une étude de risques (ex : élaborer la politique de sécurité d'un organisme, faire un cahier des charges pour un nouveau système, corriger des problèmes identifiés) ✓ Il exprime les prérequis au lancement d'une étude et les éventuelles limitations d'une étude ✓ Il explique comment intégrer l'étude des risques dans un cycle de développement d'un projet ✓ Il explique les caractéristiques qui permettront à une étude d'être réutilisable (voir reproductible)
Atelier 1 – Cadrage et socle de sécurité	8. Comprendre à quoi sert l'atelier 9. Connaître le résultat attendu 10. Savoir atteindre le résultat attendu	✓ Il explique l'atelier (cadre de l'étude, périmètre métier et technique, événements redoutés, socle de sécurité) ✓ Il décrit et justifie un événement redouté et son estimation en termes de gravité ✓ Il explique comment évaluer le socle de sécurité et les suites possibles de cette évaluation ✓ Il explique que des mesures peuvent d'ores-et-déjà alimenter le plan d'action en fournissant des exemples ✓ Il explique que l'atelier permet d'identifier les éléments utiles à la suite de l'étude
Atelier 2 – Sources de risques	11. Comprendre à quoi sert l'atelier 12. Connaître le résultat attendu 13. Savoir atteindre le résultat attendu	✓ Il explique l'atelier (sources de risques et objectifs visés, évaluation et sélection des couples jugés prioritaires) ✓ Il explique comment il réalise la typologie des sources de risques par rapport au contexte de l'étude ✓ Il décrit et justifie un couple source de risques / objectif(s) visé(s) ✓ Il explique que des mesures peuvent d'ores-et-déjà alimenter le plan d'action et fournit des exemples
Atelier 3 – Scénarios stratégiques	14. Comprendre à quoi sert l'atelier 15. Connaître le résultat attendu 16. Savoir atteindre le résultat attendu	✓ Il explique l'atelier (cartographie de menace numérique, scénarios stratégiques, mesures sur l'écosystème) ✓ Il présente un écosystème et décrit des critères d'identification des parties prenantes (notamment lorsqu'elles sont internes à l'organisme) ✓ Il décrit et justifie un scénario stratégique ✓ Il explique que des mesures peuvent d'ores-et-déjà alimenter le plan d'action et fournit des exemples
Atelier 4 – Scénarios opérationnels	17. Comprendre à quoi sert l'atelier 18. Connaître le résultat attendu 19. Savoir atteindre le résultat attendu	✓ Il explique l'atelier (scénarios opérationnels, estimation de la vraisemblance) ✓ Il décrit et justifie un scénario opérationnel et son estimation en termes de vraisemblance ✓ Il explique que des mesures peuvent d'ores-et-déjà alimenter le plan d'action et fournit des exemples
Atelier 5 – Traitement du risque	20. Comprendre à quoi sert l'atelier 21. Connaître le résultat attendu 22. Savoir atteindre le résultat attendu	✓ Il explique comment déterminer la gravité et la vraisemblance d'un risque à partir des éléments précédents ✓ Il explique les différentes options de traitement des risques ✓ Il explique et illustre des mesures complémentaires à celles identifiées lors du reste de l'étude ✓ Il présente les risques résiduels de manière compréhensible (c'est-à-dire en justifiant leur évaluation) ✓ Il présente des manières de suivre la mise en œuvre et les risques résiduels

Critère	Exigences relatives aux compétences	Exemples de points de contrôle de l'évaluation du candidat
3 Exigences relatives à la pratique de la méthode		
L'apprentissage de la méthode	23. Avoir été formé à l'utilisation de la méthode	✓ Il a suivi une formation reconnue (ex : formation dispensée par un formateur signataire de la Charte du formateur EBIOS *Risk Manager*, centre de formation de l'ANSSI, formation labellisée SecNum*Edu*-FC)
La sensibilisation	24. Avoir animé des sessions d'information à la méthode	✓ Il indique la nature de son auditoire et les messages principaux à mettre en adéquation avec celle-ci
L'organisation d'une étude	25. Savoir organiser une étude en guidant le commanditaire sur les rôles et réunions à organiser	✓ Il décrit les prérequis au lancement d'une étude (communication, outillage, sécurité, contraintes) ✓ Il décrit les acteurs dont il a besoin durant l'étude ✓ Il décrit les différentes étapes de l'étude et donne des éléments pour calculer la durée (la charge)
Les entretiens (recueil des informations)	26. Savoir conduire des entretiens pour obtenir des informations 27. Savoir s'adapter à la culture de l'organisme (ex : vocabulaire)	✓ Il adapte son vocabulaire et ses explications aux parties prenantes ✓ Il obtient les informations qui lui sont nécessaires (ex : identifier les impacts d'un événement redouté lié au contexte de l'étude de cas) ✓ Il explique comment il peut aider à l'arbitrage des choix dans un atelier (ex : choix des échelles d'impacts, choix des évènements redoutés, pertinence des sources de risques, appréciation des parties prenantes, choix des scénarios à analyser, choix de la technique d'estimation de la vraisemblance), et montre sa compréhension des impacts de ces choix dans la suite de l'étude (ex : entropie, appréciation des risques, représentation des risques)
Les réunions	28. Connaître les techniques de conduite de réunion 29. Avoir une expérience significative de conduite de réunion	✓ Il mentionne les informations indispensables à la conduite de réunion : ordre du jour préalable, énoncé de l'objectif, obtention de l'accord des participants, recadrage selon l'objectif, conclusion récapitulant des résultats atteints, *etc*. ✓ Il montre son expérience en matière de conduite de réunion
Le choix du niveau de détail	30. Savoir choisir le niveau de détail d'une étude	✓ Il explique que l'étude doit être adaptée selon son but et les livrables attendus ✓ Il cite des exemples liés au contexte d'une étude de cas qui montrent le niveau de détail choisi
La mise en œuvre d'études	31. Avoir suivi le déroulement d'études dans leur intégralité, par exemple en tant que maîtrise d'ouvrage ou assistance à maîtrise d'ouvrage 32. Avoir réalisé des études dans leur intégralité	✓ Il a mené au moins une étude ou il a suivi un nombre significatif d'études
L'obtention d'informations	33. Savoir identifier les informations nécessaires pour mener une étude 34. Connaître les types de fonctions à impliquer selon les activités de la méthode 35. Savoir analyser et utiliser les informations obtenues	✓ Il cite les documents qu'il peut exploiter et explique en quoi ils vont servir dans le cadre d'une étude de cas ✓ Il cite les personnes ou fonctions qu'il peut impliquer et explique leur rôle dans le cadre de l'étude de cas
Le travail en équipe	36. Savoir travailler en équipe	✓ Il explique les apports de l'implication de diverses parties prenantes ✓ Il évoque des exemples vécus de travaux en équipe
L'exploitation des bases de connaissances	37. Savoir utiliser et ajuster les bases de connaissances	✓ Il présente différentes bases de connaissances utilisables ✓ Il explique comment il les a déjà utilisées et ajustées
L'obtention d'arbitrages	38. Savoir préparer et obtenir des arbitrages tout au long d'une étude	✓ Il décrit son expérience en préparation et obtention d'arbitrage ✓ Il explique qui peut décider des choix à effectuer dans le cadre de différents ateliers

Critère	Exigences relatives aux compétences	Exemples de points de contrôle de l'évaluation du candidat
L'adaptation à la maturité de l'organisme	39. Savoir proposer des mesures de sécurité raisonnables selon la réalité de l'organisme (selon sa maturité)	✓ Il détermine des mesures de sécurité pertinentes vis-à-vis du contexte d'une étude de cas pour un risque donné, et justifie ses choix
L'implication et la responsabilisation des acteurs	40. Savoir impliquer et responsabiliser les parties prenantes	✓ Il utilise les éléments de langage des parties prenantes ✓ Il fait porter les choix par les parties prenantes (ce n'est pas lui qui décide)
La production de livrables	41. Savoir expliquer les différents types de livrables principalement produits et leurs finalités 42. Savoir produire des documents livrables adaptés à partir d'une étude	✓ Il explique pourquoi il est important d'adapter ses livrables ✓ Il décrit différents livrables selon différents contextes
L'obtention de validations	43. Savoir obtenir des validations	✓ Il fournit les informations nécessaires à la compréhension (de manière adaptée à l'auditoire) et à la prise de décision (il justifie les choix, présente les risques résiduels, *etc*.) ✓ Il explique ce qu'il fait valider ou non et le justifie
L'explication des conclusions	44. Savoir présenter une communication au niveau décisionnel 45. Avoir présenté les conclusions d'une étude à un niveau décisionnel	✓ Il explique comment il va présenter plusieurs dizaines ou centaines de risques à une direction (classement pertinent, évocation uniquement des principaux risques, critères de gestion utilisés, exploitation de la gravité et de la vraisemblance, *etc*.) ✓ Il justifie ses choix

Références

[Référentiel de compétences]	*Certification EBIOS Risk Manager – Référentiel de compétences*, version du 1er août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-Competences.pdf
[Exigences relatives au schéma de certification]	*Certification EBIOS Risk Manager – Exigences relatives au schéma*, version du 1er août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-ExigencesSchema.pdf
[Exigences relatives aux compétences]	*Certification EBIOS Risk Manager – Exigences relatives aux compétences*, version du 1er août 2020, Club EBIOS. https://club-ebios.org/site/wp-content/uploads/site-documents/ClubEBIOS-Certification-Referentiel-ExigencesCompetences.pdf