Dispositif particulier

Certification «Security Risk Manager ISO/IEC 27005»

Table des matières

1. Description de la certification « Sécurity Risk Manager ISO/IEC 27005»

1.1 Intitulé de la certification

Security Risk Manager ISO/IEC 27005 est délivré par Bestcertifs en application des exigences de la norme ISO/IEC 17024 : 2012 Évaluation de la conformité — Exigences générales pour les organismes de certification procédant à la certification de personnes.

1.2 Objectif de la certification

L'objectif principal de cette certification est de valider les compétences des professionnels capables d'identifier, évaluer et traiter les risques auxquels est soumis le système d'information de façon à préserver les activités essentielles de l'entreprise en s'appuyant sur la norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

1.3 Périmètre de la certification

Toutes les informations détenues par une entreprise sont exposées à des menaces d'attaques, d'erreur, d'événements naturels et sont exposées à des vulnérabilités inhérentes à leur utilisation.

Le Système d'Information peut être de nature complexe changeante fortement interconnecté et exposé à une menace qui revêt des formes multiples et variables dans le temps. Les pirates informatiques représentent un risque très important pour les entreprises, quel que soit leur taille.

Comment se protéger dans la durée ?

Les organisations qui souhaitent se protéger peuvent simuler des intrusions pour évaluer à posteriori la vulnérabilité du système d'information. Ils sont peu onéreux mais n'offrent aucune garanties quant aux risques résiduels du système testé.

Pour s'assurer de réduire les risques résiduels, il y a d'autres méthodes qui sont à mettre en œuvre tout au long du développement du système et qui s'appuie sur l'analyse de risques.

Une famille de norme, appelée ISO 27000, donne une approche méthodologique pour améliorer de façon constante la sécurité du système d'information. En utilisant ces normes on crée un système de management de la sécurité de l'information (SMSI).

L'ISO 27001 décrit les exigences à mettre en place pour créer un système de management. L'ISO 27005 complète l'ISO 27001 pour guider la mise en place du management des risques appliqué au système d'information.

La norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information préconise au sein du SMSI une démarche continu et itérative basée sur 2 activités essentielles qui s'adaptent particulièrement bien aux enjeux actuels : l'appréciation du risque et le traitement du risque.

Il est à noter que l'ISO 27005 ne fournit pas de modèle d'analyse des risques. Il existe plusieurs méthodologies dont la méthode e-bios qui est recommandée par l'ANSSI[1].

Ainsi, compte tenu du contexte spécifique, il est devenu nécessaire pour toute entreprise aujourd'hui de mettre à jour en continu son dispositif de sécurité de l'information en s'appuyant sur :

- sur les normes de la famille ISO 27000 et plus précisément de l'ISO 27005

- l'utilisation d'une méthodologie d'analyse des risques telle que e-bios

- un retour d'expérience s'appuyant sur une analyse de cas réels

Dans ce cadre la mission du Security Risk Manager est d'identifier, évaluer et traiter les risques auxquels est soumis le système d'information de façon à préserver les activités essentielles de l'entreprise en s'appuyant sur la norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

1.4 A qui s'adresse cette certification

Public Visé :

- Professionnels et/ou Auditeurs de la Sécurité de l'Information souhaitant certifier qu'ils sont capables de préparer, réaliser des analyses de risques menées en conformité avec la norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information, en particulier dans le cadre d'un SMSI conforme à la norme NF EN ISO/CEI 27001 : 2017;

- Consultants désirant certifier qu'ils sont capables de maîtriser les principes et le processus d'une analyse de risque selon la norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information;

- Toutes personnes, quelles que soient leurs postes dans l'entreprise en relation avec le Système de Management de la Sécurité de l'Information (SMSI), désireuses de prouver qu'elles sont capables d'avoir des responsabilités dans la maîtrise des risques d'un système d'informations selon la norme NF EN ISO/IEC 27005 : 2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information (Responsable de la Sécurité des Systèmes d'Information et Responsable de la Conformité)

1. 5 Candidature à la certification et à l'examen

Pour candidater à la certification, il sera demandé

- De compléter le formulaire de candidature disponible sur la page de description de la certification sur le site www.bestcertifs.com

- De téléverser un CV justifiant d'une expérience d'au moins trois ans dans la gestion des systèmes d'information et métiers rattachés au système d'information

- de téléverser un fichier numérisé d'une pièce d'identité légale en cours de validité comprenant une photo, les nom prénom et date de naissance, rédigée en alphabet latin ; cette pièce sera la pièce demandée pour la vérification de l'identité lors du passage de

1 https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

l'Examen de certification (carte d'identité, passeport, permis de conduire …). A défaut, le numéro de passeport/carte d'identité et le nom et prénom du candidat.
- Le cas échéant, le candidat pourra demander une adaptation de l'Examen en cas de handicap: il en fait la demande dans dossier de candidature. Les demandes seront traitées au cas par cas.

Pour candidater à l'examen, vous pouvez passer par un organisme de formation qualifié qui prépare aux examens de la certification ou réaliser vous même votre inscription sur le site de bestcertifs. Pour passer cet examen, nous vous conseillons néanmoins d'être titulaire d'un diplôme de niveau minimum Bac+2.

1.6 Règles d'usages de la certification

Validité – Eléments figurant sur le certificat – Suspension et retrait – Abandon du certificat- Réduction du périmètre de la certification Voir Procédure de certification paragraphe 5.3. : cliquez ici

1.7 Candidature pour le renouvellement de la certification

Pour candidater au renouvellement, il faudra produire les éléments suivants :

- De compléter le formulaire de candidature disponible sur la page de description de la certification sur le site de bestcertifs
- de téléverser un fichier numérisé d'une pièce d'identité légale en cours de validité comprenant une photo, les nom prénom et date de naissance, rédigée en alphabet latin ; cette pièce sera la pièce demandée pour la vérification de l'identité lors du passage de l'Examen de certification (carte d'identité, passeport, permis de conduire …). A défaut, le numéro de passeport/carte d'identité et le nom et prénom du candidat.

Le renouvellement se fait pour une période de 3 ans.

1.8 Missions, tâches, compétences, critères d'évaluation

La réalisation de la certification est le résultat d'un travail d'ingénierie de formation qui part de la description des activités et tâches réalisées par un professionnel en charge de l'évaluation des risques auxquels sont soumis les systèmes d'informations de l'entreprise.

Activités, tâches compétences

Activités	Tâches	Compétences
Définir le périmètre de l'analyse de risques	Préciser la ou les missions sensibles de l'organisation	C1. Identifier les processus métiers sensibles et stratégiques et leur système d'information associé en s'appuyant sur une analyse SWOT de l'environnement et de l'entreprise afin de garantir la cohérence des décisions de traitements des risques avec la stratégie de l'entreprise
	Caractériser l'environnement humain, sociétal, technique, physique dans lequel évolue l'entreprise	
	Identifier processus métiers associées en lien avec la ou les missions sensibles	
	Identifier le ou les systèmes d'information supportant les processus et l'information sensibles	C2. Délimiter le domaine d'application (périmètre d'action) sur lequel s'exerce l'analyse de risque en synthétisant toutes les informations collectées issus de groupe de travail collaboratifs et de la documentation de l'entreprise afin de définir la stratégie d'évaluation et de traitement des risques
	Déterminer les critères de probabilité, d'occurrence et d'impact d'évaluation des risques	
	Déterminer les critères de probabilité, d'occurrence et d'impact d'évaluation des risques	
	Rédiger un rapport définissant le périmètre et les critères de risques	
Apprécier les risques	Identifier les risques	C3. Construire et hiérarchiser des scenarii de dysfonctionnements ou d'agressions permettant aux risques identifiés de survenir afin de valider les scenarii
	Analyser les risques , identifier les causes et les conséquences des risques identifiés	
	Evaluer les risques	
	Composer une cartographie des risques permettant de les prioriser	
	Préparer les éléments de décision quant au traitement des risques	
Traiter les risques	Trouver tous les moyens à mettre en place pour réduire les risques : plan, technique, organisation	C4. Elaborer les plans de traitement des risques (intégrant l'impact, la probalité et les risques résiduels) en s'appuyant sur l'analyse des scénarii afin de permettre à la direction de l'entreprise de choisir les plus pertinents au regard de la stratégie de l'entreprise
	Estimer les bénéfices et la rentabilité des différents traitements	
	Réévaluer les risques résiduels après traitement	
	Etablir les indicateurs qui permettront la mesure de la performance du traitement	
	Présenter un plan de traitement des risques à la Direction dans le but de provoquer une décision	
Garantir que la gestion risques est une des activités essentielles de l'entreprise	S'assurer de la bonne mise en œuvre du plan de traitement	C5. Accompagner l'entreprise dans la mise en œuvre du plan de traitement en s'appuyant sur des indicateurs de suivi des dysfonctionnements et en collectant de retours d'expérience afin de s'assurer de son efficacité dans le temps
	S'assurer de l'efficacité du plan de traitement (indicateurs et suivi des dysfonctionnements)	
	Suivre et animer le retour d'expérience	C6. Favoriser une culture de la gestion du risque lié au système d'information dans l'organisation en facilitant les remontées d'incidents de sécurité de l'information et leur analyse afin de pérenniser les bénéfices obtenus de la démarche
	Fédérer les analyses d'incidents	

Référentiels de compétences et d'évaluation

Compétences	Critères d'évaluation
C1. Identifier les processus métiers sensibles et stratégiques et leur système d'information associé en s'appuyant sur une analyse SWOT de l'environnement et de l'entreprise afin de garantir la cohérence des décisions de traitements des risques avec la stratégie de l'entreprise	Cr1.Le choix des processus est justifié : il s'appuie sur la caractérisation de l'environnement sur les plans humain, sociétal, technique ou physique en terme de menaces et opportunités ; les processus métiers sont clairement reliés à leur système d'information ; les personnes ressources pertinentes ont été associées
C2. Délimiter le domaine d'application (périmètre d'action) sur lequel s'exerce l'analyse de risque en synthétisant toutes les informations collectées issus de groupe de travail collaboratifs et de la documentation de l'entreprise afin de définir la stratégie d'évaluation et de traitement des risques	Cr2. Les processus et les systèmes d'information (actifs informatiques) concernés sont déterminés ; leur choix est justifié et en lien avec les priorités de l'entreprise Les échelles de mesure des risques sont établis sur la base de critères qualitatifs et quantitatifs
C3 : Construire et hiérarchiser par criticité des scenarii de dysfonctionnement ou d'agression en s'appuyant sur les personnes ressources compétentes afin de retenir les scénarii les plus critiques en fonction de leur probabilité et de leurs impacts	Les scenarii retenus sont pertinents : ils sont clairement associés à des risques ; ils couvrent une majorité de risques ; ils sont fidèles et cohérents avec les enjeux des métiers ; ils proposent une évaluation chiffrée des impacts ou de leur probabilité
C4. Elaborer les plans de traitement des risques (intégrant l'impact, la probalité et les risques résiduels) en s'appuyant sur l'analyse des scénarii afin de permettre à la direction de l'entreprise de choisir les plus pertinents au regard de la stratégie de l'entreprise	Cr4. Les plan de traitement des risques sont complets et efficaces : ils couvrent complètement les enjeux de l'organisation ; les solutions proposées sont réalistes et pratiques ; elles sont d'ordre technique, organisationnel et comportemental ; elles sont hiérachisées en fonction de la criticité du risque et du nombre de risques couverts ; elles sont articulées de façon cohérente ; les indicateurs de performance sont limités à 10 ; les seuils sont définis et leur franchissement entraîne une réaction
C5. Accompagner l'entreprise dans la mise en œuvre du plan de traitement en s'appuyant sur des indicateurs de suivi des dysfonctionnements et en collectant de retours d'expérience afin de s'assurer de son efficacité dans le temps	Cr5. L'accompagnement est structuré : les contrôles sont systématiques ; les actions de formation et d'information sont formalisées ; les outils de suivi sont identifiés (tableaux de bord, documentation, fiches pratiques, bulletins d'information, brieffing…)
C6. Favoriser une culture de la gestion du risque lié au système d'information dans l'organisation en facilitant les remontées d'incidents de sécurité de l'information et leur analyse afin de pérenniser les bénéfices obtenus de la démarche	Cr6. La culture de gestion des risques est intégrée : Les salariés sont proactifs dans la gestion des risques ; ils rendent compte des dysfonctionnements et d'incidents évités ; la gestion des risques fait partie des processus métiers de l'entreprise ; des mesures liées à la sécurité de l'information sont réalisées de manière systématiques ; des mesures correctrices sont planifiées et leur efficacité est mesurée

1.9 Modalités de l’examen initial et de renouvellement

L’examen initial est réalisé par le passage de 2 questionnaires à choix multiples relatives à la mise en place d’un audit des Systèmes de Management de la Sécurité de l’Information sur une plateforme LMS BESTCERTIF (https://exam.bestcertifs.com/) en mode supervisé par un surveillant:

1. Un questionnaire de 30 questions se rapportant aux connaissances

2. Un questionnaire de 50 questions se rapportant à une étude de cas complexe qui portera sur une entreprise et présentera le contexte spécifique, les particularités de l’entreprise, les enjeux et tous les éléments détaillés de l’entreprise

L’évaluation se fait à distance selon les modalités décrites dans la Procédure de Certification au paragraphe 4.3. 1 Méthode d’évaluation

Durée : 2h00

Score minimum : obtenir 56 points sur 80

L’examen de renouvellement est réalisé par le passage d’un questionnaire à choix multiples relatif à la mise en place d’un audit des Systèmes de Management de la Sécurité de l’Information sur une plateforme LMS BESTCERTIF (https://exam.bestcertifs.com/)

L’évaluation se fait à distance selon les modalités décrites dans la Procédure de Certification au paragraphe 4.3. 1 Méthode d’évaluation

Durée : 1h00

Score minimum : obtenir 35 points sur 50

Le processus de re-certification peut prendre jusqu'à un mois.

1.10 Coût de la certification et du renouvellement

Le prix de la certification s’élève à 399 euros et son renouvellement à 175 euros

2. Procédure de certification

Voir la procédure de certification sur le site https://www.bestcertifs.com/ et en cliquant ici .