J 24 IZOGOOD® 27001

DÉCRYPTER L'ISO 27001 EN S'AMUSANT

LIVRET DU JOUEUR

Table des matières

1. Règles du jeu
2. Glossaire
3. Risques
4. QCM
5. Pratiques
6. Cas

1. Règles du jeu

Le jeu est prévu pour une personne, mais rien n'empêche de jouer en petit groupe, cela sera bien plus ludique.

Le jeu est compatible avec les versions récentes des navigateurs Web. Autrement le jeu peut être lent.

Une séance de jeu dure en moyenne entre une demi-heure et 2 – 3 heures. Vous pouvez jouer autant de fois que vous souhaitez pendant votre accès de 60 jours et assimiler les connaissances liées à la norme ISO 27001.

Le but du jeu est d'arriver le plus vite à la dernière case (Arrivée). 

Les exigences de la norme et des commentaires sont sur cette page. Un quiz gratuit sur les exigences de la norme ISO 27001 est fourni au début de la page. Cela vous permet de découvrir, décrypter et se familiariser avec les exigences de la norme.

Avoir à portée de main un exemplaire de la norme ISO 27001 (non fourni avec le jeu) est un prérequis.

Le fond d'écran du jeu est une ville et un parcours de la voiture.

En haut à gauche vous avez une horloge avec le temps écoulé. En haut à droite vous avez une aide et un bouton pour quitter le jeu.

En bas à gauche vous avez un bouton pour couper le son. En bas au milieu vous avez le total d'étoiles gagnées ★. En bas à droite vous avez un bouton avec un lien vers la page des exigences de la norme ISO 27001.

Au début la voiture est stationnée à la case Départ. 

Le jeu débute en cliquant sur le bouton COMMENCER LE JEU.

La séquence des cases (types des cartes) est la suivante :

- RISQUE - menace ou opportunité – argent 
- QCM - questionnaire à choix multiples – vert 
- PRATIQUE - bonne pratique ou écart à éviter – orange 
- CAS – situation, défi et solutions – bleu 

Vous avez aussi 4 cases Maintenance  et 4 cases boîtes de Pandore  .

Chaque type de case inclut 50 questions (cartes), la réponse de chaque carte est liée à un paragraphe de la norme ISO 27001 version 2022.

Chaque carte est montrée avec les étapes suivantes :

- étape 1. Le dos de carte avec le type de carte, le numéro (de 1 à 50) et le nombre d'étoiles (de une à trois) en bleu, blanc et rouge ★, ☆☆, ★★★
- étape 2. Le type de carte, son numéro, la question (par exemple : Est-ce que l'affirmation suivante est plutôt une menace ou une opportunité ?), l'affirmation (par exemple : Le domaine d'application du SMSI décrit les activités principales de l'entreprise) et l'étoile
- étape 3. Les réponses (une ou plusieurs réponses correctes sont possibles) un émoji vert (pour **toutes** les bonnes réponses) et un émoji rouge (pour une mauvaise réponse)
- étape 4. Le paragraphe de la norme et un commentaire pour la bonne réponse ou un commentaire pour la mauvaise réponse

La voiture démarre et arrive sur la case Risque .

Le numéro de la carte est aléatoire. En relation avec la difficulté de la question les étoiles sont une, deux ou trois.

Si vous avez deviné la bonne réponse la voiture avance autant de cases que la question contient d'étoiles.

Si vous n'avez pas deviné la bonne réponse (ou répondu partiellement) la voiture cale sur la même case et la carte suivante sera du même type.

Si vous tombez sur une case Maintenance ou une case boîte de Pandore , vous pouvez avoir de la chance ou de la malchance. Du coffre de la voiture ou de la boîte de Pandore sort une carte aléatoire chance ou malchance. La chance c'est une carte Joker et votre voiture avance de 3 cases. Si c'est la carte Malchance qui sort du coffre ou de la boîte, votre voiture recule de 3 cases.

Si une deuxième personne est à côté de vous et elle a imprimé le présent livret, elle peut augmenter la difficulté du jeu en posant, entre autres, ces questions :

- Quel est l'article et le paragraphe de la norme en lien avec la question posée ?
- Pouvez-vous donner un exemple de votre département en lien avec cette question ?

Quand vous êtes arrivé pour la première fois à la case Arrivée vous pouvez télécharger votre Attestation de participation au jeu IZOGOOD® 27001.

Vous pouvez aussi voir le suivi des résultats du jeu :

- le nombre d'étoiles gagnées
- la date et l'heure chaque fois que vous avez joué
- le temps passé

Les objectifs pédagogiques du jeu sont de permettre à chaque joueur :

- d'identifier si un risque est plutôt une menace ou une opportunité
- d'enrichir ses connaissances sur les exigences de la norme grâce aux QCM
- de deviner si une affirmation est plutôt une bonne pratique ou un écart à éviter
- d'étudier pour chaque cas proposé la situation, le défi et de trouver la bonne solution (une ou plusieurs solutions correctes sont possibles)
- de décrypter les articles et paragraphes de la norme et d'assimiler les exigences

Certaines questions comportent un soupçon d'humour (même si le chef a oublié de le dire).

Détendez-vous, ce n'est qu'un jeu. 

Un parti pris est inévitable quant aux « bonnes réponses » à retenir, en particulier pour les cartes RISQUE ou PRATIQUE.

Voici ci-dessous un exemple :

Carte RISQUE 01. L'affirmation suivante est-elle plutôt une menace ou une opportunité ? « **Le plus important est que la stratégie de l'entreprise ait été établie dans le passé »**

On pourrait répondre que c'est une menace ou une opportunité mais cela dépend de la date à laquelle la stratégie a été définie.

Si vous répondez que c'est une menace, vous avez raison car il n'est pas précisé quand la précédente stratégie a été élaborée (il y a un an, il y a 10 ans). Il y a donc une information manquante. Mais vous pourriez répondre que c'est une opportunité car vous pensez que « dans le passé » veux dire 2 à 3 ans.

Ainsi, les réponses et la pertinence des commentaires présentés sont contestables, en fin de compte la vérité est parfois relative.

Le jeu IZOGOOD a été créé et réalisé avec beaucoup d'attention. Merci d'avance de nous communiquer les éventuels points de progrès que vous avez identifié via ce lien : https://www.pqb.fr/contact.php

2. Glossaire

Le début de la sagesse est la définition des termes. Socrate

Certains termes spécifiques :

Actif : *tout élément ayant de la valeur pour l'organisation*
Action corrective : *action pour éliminer les causes d'une non-conformité ou tout autre événement indésirable et empêcher leur réapparition*
Amélioration continue : *processus continu permettant d'améliorer la performance globale de l'entreprise*
Approche processus : *management par les processus pour mieux satisfaire les clients, améliorer l'efficacité de tous les processus et augmenter l'efficience globale*
Audit : *examen méthodique et indépendant en vue de déterminer si les activités et les résultats satisfont aux dispositions préétablies et sont aptes à atteindre les objectifs*
Client : *celui qui reçoit un produit*
Confidentialité : *propriété d'une information pouvant être dévoilée seulement aux personnes autorisées*
Conformité : *satisfaction d'une exigence spécifiée*
Cryptographie : *activités de protection de la confidentialité d'une information à l'aide de codification et de décodification*
Déclaration d'applicabilité (DdA) : *document décrivant les objectifs et les mesures de sécurité*
Dérogation (après production) : *autorisation écrite de livrer un produit non conforme*
Direction : *groupe ou personnes chargées de la gestion au plus haut niveau de l'entreprise*
Document : *tout support permettant le traitement d'une information*
Efficacité : *capacité de réalisation des activités planifiées avec le minimum d'efforts*
Efficience : *rapport financier entre le résultat obtenu et les ressources utilisées*
Entreprise (organisation) : *structure qui satisfait un besoin*
Exigence : *besoin ou attente implicite ou explicite*
Indicateur : *valeur d'un paramètre, associé à un objectif, permettant de façon objective d'en mesurer l'efficacité*
Inspection : *actions de mesures, d'essais et d'examens d'un produit, service, processus ou matériel pour déterminer le respect des exigences*
Intégrité : *propriété d'une information d'être non altérée*
Management de la sécurité de l'information : *activités permettant de maîtriser une entreprise en matière de sécurité de l'information*
Non-conformité : *non-satisfaction d'une exigence spécifiée*
Objectif de sécurité de l'information : *but mesurable à atteindre lié à la sécurité de l'information*
Partie prenante : *personne, groupe ou organisation pouvant affecter ou être affecté par une entreprise*
Performance : *résultats mesurables et attendus du système de management*
PESTEL : *Politique, Économique, Sociologique, Technologique, Écologique, Légal. Analyse permettant d'identifier l'influence des facteurs externes*
Prestataire externe (fournisseur) : *celui qui procure un produit*
Preuve d'audit : *données factuelles par rapport aux critères d'audit dont la véracité peut être démontrée*
Processus : *activités qui transforment des éléments d'entrée en éléments de sortie*
Produit (ou service) : *tout résultat d'un processus ou d'une activité*
Qualité : *aptitude à satisfaire aux exigences*
Revue : *examen d'un dossier, d'un produit, d'un processus afin de vérifier l'atteinte des objectifs fixés*
Revue de direction : *examen périodique réalisé par la direction du système de management pour son amélioration continue*

Risque : *vraisemblance d'apparition d'une menace ou d'une opportunité*
Satisfaction du client : *objectif prioritaire de chaque système de management à la satisfaction des exigences client*
Sauvegarde : *copie de données afin d'archiver et protéger contre la perte*
Sécurité de l'information : *mesures permettant de protéger la confidentialité, l'intégrité et la disponibilité de l'information*
SI : *sécurité de l'information*
SMSI : *système de management de la sécurité de l'information*
SWOT : *Strengths, Weaknesses, Opportunities, Threats ou forces, faiblesses, opportunités, menaces. Outil pour structurer une analyse des risques*
Système de management : *ensemble de processus permettant d'atteindre les objectifs*
Traçabilité *: aptitude à mémoriser ou restituer tout ou partie d'une trace des fonctions exécutées*
Vérification : *examen périodique de la conformité d'un processus, d'un produit, service ou matériel*
Validation : *notice que l'application d'un processus, produit, service ou matériel permet d'atteindre les résultats escomptés*
VLAN : *Virtual Local Area Network, Réseau local virtuel*

Remarque 1 : le mot anglais "control" a plusieurs sens. Il peut être traduit par maîtrise, autorité, commande, gestion, contrôle, surveillance, inspection. Pour éviter des malentendus notre préférence est pour maîtrise et inspection au détriment de contrôle

Remarque 2 : entre processus et procédé notre préférence est pour processus (en anglais "process")

Remarque 3 : organisme (en anglais organization) est le terme utilisé dans l'ISO 27001 pour l'entité entre le prestataire externe (fournisseur) et le client. Organisation est utilisé par l'ISO 26000, l'EFQM, l'ONU et beaucoup d'autres. Pour éviter la confusion avec organisme de certification notre préférence est pour le terme entreprise

Remarque 4 : un document peut être présenté comme une information documentée que l'on doit tenir à jour (procédure) ou conserver (enregistrement)

Remarque 5 : le cycle PDCA (en anglais Plan, Do, Check, Act) nous traduisons par Planifier, Dérouler, Comparer, Agir

3. RISQUES 

Question récurrente : Est-ce que l'affirmation suivante est plutôt une menace ou une opportunité ?

RISQUE 01 Le plus important est que la stratégie de l'entreprise ait été établie dans le passé
Menace § 4.1 ★★★
Tous les trois ans en moyenne, il convient de vérifier l'adéquation de la stratégie au contexte de l'entreprise, aux attentes et besoins des parties prenantes. Menace car la date de l'élaboration de la stratégie n'est pas précisée

RISQUE 02 Le contexte de l'entreprise est un élément qui peut être pris en considération (même si le chef a oublié de le dire)
Menace § 4.1 ☆☆
C'est une exigence de la norme et c'est incontournable. Cela fait partie des premiers travaux à réaliser puisque la validation de la stratégie de l'entreprise en dépend

RISQUE 03 Chercher à anticiper l'évolution des attentes du client est du temps perdu (si c'est le chef qui le dit)
Menace § 4.2 ★
L'objectif de l'entreprise étant de satisfaire durablement ses clients, connaître les évolutions des attentes est un facteur clé de succès pour l'avenir

RISQUE 04 On peut essayer de respecter les exigences légales (si le chef est d'accord)
Menace § 4.2 ★
On doit respecter strictement les exigences légales

RISQUE 05 Le domaine d'application du SMSI décrit les activités principales de l'entreprise
Opportunité § 4.3 ☆☆
Décrire le domaine d'application du SMSI, c'est délimiter les entités et les activités concernées. Les exclusions doivent être précisées

RISQUE 06 Promouvoir en interne la cartographie des processus (car le chef a dit de nous débrouiller)
Opportunité § 4.4 ★
C'est une opportunité de faire connaître à chaque personne en interne la cartographie des processus. Ceci permet à chacun de se situer dans le fonctionnement global de l'entreprise et dans les relations client fournisseur avec les autres processus

RISQUE 07 L'engagement de la direction ne contient pas des objectifs établis
Menace § 5.1 ☆☆
La direction fait preuve de leadership et affirme son engagement, entre autres, en s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information

RISQUE 08 La direction détermine et tient à jour la politique de sécurité de l'information en cohérence avec l'orientation stratégique de l'entreprise
Opportunité § 5.2 ☆☆
La politique de sécurité de l'information est appropriée à la mission (orientation stratégique) de l'entreprise