Livre blanc

ISO 9001 et le management des risques

Se poser les bonnes questions

Le management des risques, autrement dit l'approche par les « risques et opportunités », est une exigence nouvelle de la norme ISO 9001:2015. Il s'agit là d'un concept difficile à appréhender et le grand danger pour les qualiticiens est d'élaborer une organisation complexe et sans grande valeur ajoutée qui pourrait décrédibiliser les démarches qualité et les normes ISO aux yeux des directions générales.

Il est donc essentiel, avant de répondre à cette exigence, d'en comprendre les fondements et les principes afin de permettre la mise en place de dispositions au juste nécessaire. L'approche par les risques permet d'améliorer les performances des organismes qui les pratiquent. C'est là son intérêt majeur.

Les questions (et les réponses) ci-dessous sont celles que se posent le plus souvent les responsables chargés de l'efficacité et de l'efficience des démarches qualité.

Pour des raisons de simplicité, les textes qui suivent ne traitent que de la notion de risques et non de celle d'opportunités.

CHAPITRE

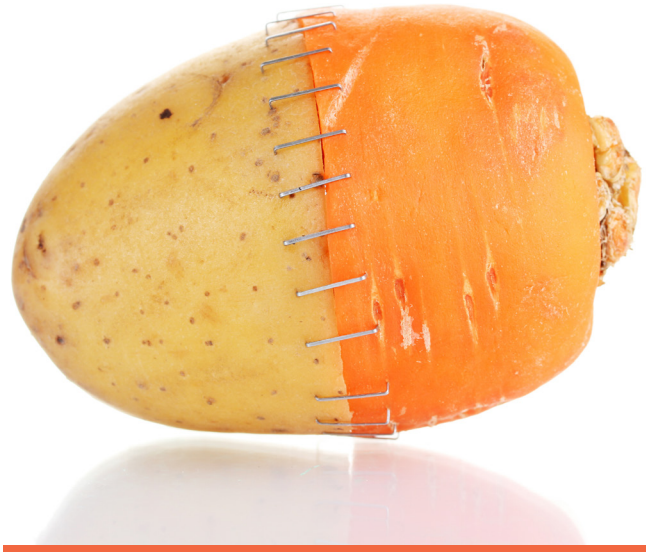
1

APPROCHE GÉNÉRALE : COMPRENDRE LES ENJEUX

1 Faut-il mettre en place une approche risque intégrée qualité, sécurité et environnement ?

Rien ne l'interdit mais ce n'est pas la manière la plus efficace de répondre aux exigences des référentiels concernés. D'abord on risque de se lancer dans une opération compliquée et difficile à mettre en place. Ensuite les finalités des trois modes de management (santé, environnement et qualité) sont assez différentes.

La norme ISO 9001 n'exige pas une approche pluridisciplinaire en ce qui concerne le management des risques. Si un organisme n'est pas impliqué dans une démarche relative au management de la santé et sécurité au travail et de la préservation de l'environnement, inutile de partir sur plusieurs fronts à la fois. Il y a déjà une réflexion importante à mener sur les risques qualité sans se charger, en plus, des autres catégories de risques. D'autre part, les finalités des trois typologies de management sont fondamentalement différentes. En matière de santé et sécurité au travail, l'objectif est le zéro. D'ailleurs, dans cette approche, on parle d'une première étape qui est d'identifier les dangers. Toute activité humaine peut être dangereuse pour l'être humain à des degrés différents, cela va de soi. Il est donc difficile de penser que le moindre risque peut être acceptable même si les conséquences en sont relativement faibles. Pour la préservation de l'environnement, l'objectif premier est de satisfaire à la réglementation et d'engager une dynamique d'amélioration. En ce qui concerne la qualité, la prise de risques est un facteur clé de succès et on n'y parle pas de danger. En conséquence, il est préférable, dans un organisme qui intègre les trois modes de management, de ne pas mélanger les genres. Il faut, pour chaque processus, que les pilotes identifient les résultats attendus en matière de santé et sécurité au travail puis en matière de préservation de l'environnement puis en matière de qualité. Ces analyses doivent être réalisées en trois temps et consignées dans des enregistrements différents qui permettront des suivis spécifiques et adaptés.



2

Faut-il procéder à une analyse globale des risques ou bien à des analyses par processus ?

Le référentiel ne montre pas d'exigence à ce sujet et il faut que les analyses de risques couvrent toutes les activités du management de la qualité. Cependant, l'article 4.4 intitulé « Système de management de la qualité et processus associés » mentionne à l'alinéa f) que : « …l'organisme doit déterminer les risques et opportunités… »

Il y a effectivement au moins deux manières d'aborder l'approche « risques » dans un système de management de la qualité. On peut procéder, comme on le fait généralement dans les référentiels IS0 14001 ou 45001 relatifs au management environnemental ou au management de la santé et sécurité au travail, avec une analyse globale réalisée le plus souvent par le responsable HSE. Dans notre cas, ce sera fait par le responsable qualité. On peut également procéder par processus avec une analyse des risques à caractère stratégique dans le ou les processus de management et avec une analyse des risques de type opérationnels dans les autres processus de support et de réalisation.

Personnellement, je pense que la seconde solution est préférable car elle rend la responsabilité de l'évaluation et bien entendu des actions qui en résultent aux pilotes de processus. Il faut au préalable leur apporter une méthode, de manière à ce que l'approche « risques » soit harmonisée dans toutes les activités de l'organisme. Ensuite, c'est aux pilotes de faire le travail. Il est important que le responsable qualité 2015 ne soit plus un opérationnel mais seulement un animateur et un coach. Cela va dans le sens de l'esprit de la version 2015 du référentiel 9001 qui souhaite (qui exige) que les « exigences liées au système de management de la qualité sont intégrées aux processus métiers de l'organisme » comme on peut le lire dans l'article § 5.1.1 : « Responsabilité et engagement de la direction relatifs au système de management de la qualité »

De plus, cela lui laissera plus de temps pour des tâches qui lui incombent vraiment, par exemple convaincre les personnels de tout niveau du bien-fondé du système de management de la qualité et de son intérêt.

3

Comment aborder l'approche par les risques sans complexité excessive ?

En l'abordant à travers l'identification préalable des résultats attendus. C'est d'ailleurs la définition donnée par la version 2015 de la norme ISO 9000. Un risque est un effet de l'incertitude.

Pour information, le dernier avant-projet DIS de ce référentiel était beaucoup plus précis puis qu'il expliquait que le risque était un effet de l'incertitude sur un résultat attendu. Dans la version définitive de 2015, ce sont les notes qui expliquent et détaillent cette définition.

Si l'on identifie les risques sans cette précaution préalable, non seulement il risque (!) d'y en avoir un nombre incalculable mais il est probable que les solutions décidées pour les traiter ne seront pas forcément adéquates. Pour être plus clair, je prendrai un exemple dans un EHPAD qui est une maison de retraite pour personnes dépendantes âgées. Une manière classique d'identifier les risques est de suivre les activités d'un résident tout au long d'une journée et d'identifier toutes les situations de danger qu'il peut encourir, d'évaluer ensuite les risques et les traiter. En ce qui concerne la prise des repas (déjeuner par exemple), on identifiera à coup sûr un risque d'intoxication alimentaire d'autant plus que les aînés sont des personnes relativement fragiles avec des systèmes immunitaires affaiblis par l'âge. Le niveau de ce risque sera vraisemblablement élevé dans un établissement qui dispose d'une cuisine et qui prépare les repas. Que se passerait-il alors ? Ce risque pourra être traité en supprimant la cuisine sur place et en sous-traitant cette activité à une entreprise de restauration collective qui, par expérience, maîtrise parfaitement ses procédés de productions (HACCP, respect de la chaîne de froid, choix d'ingrédients à moindre risque comme les œufs en poudre par exemple, etc.). Mais quid du service personnalisé et du bien-être des résidents, lorsqu'on sait que le repas est un moment très apprécié par les personnes âgées ?

Si l'on tient compte des résultats attendus, la recherche du plaisir à table en est un ! Si l'on est conscient de la finalité d'une maison de retraite qui doit satisfaire ses clients comme toute entreprise engagée dans des démarches qualité, si on tient compte des résultats attendus disais-je, alors cette solution ne sera pas privilégiée. Une cuisine fraîche, comme à la maison, est sans conteste plus goûteuse qu'une cuisine standardisée, même très soignée. Et puis, si les livraisons se font en plateau, comment tenir compte alors des quantités souhaitées par les résidents ? Ceux qui mangent beaucoup, ceux qui mangent très peu et qu'un plateau bien rempli va décourager.

Le traitement des risques ne doit en aucun cas dégrader la qualité des prestations offertes et de nombreuses solutions résident dans une formation des personnels et dans une plus grande implication de leur part (attention, surveillance accrue, etc.) ou bien encore dans une prise de risque partagée (avec les résidents ou leurs familles) lorsque cela est nécessaire et possible.

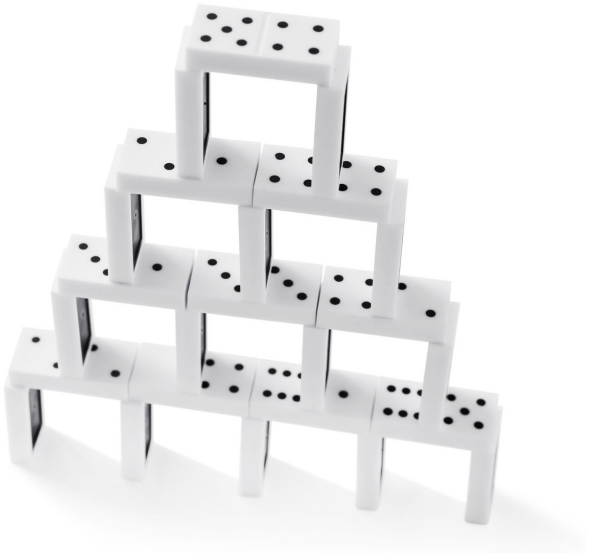
4

Doit-on utiliser une méthode pour mettre en œuvre un management des risques ?

Oui et non. Oui, car il faut manager les risques et il faut par conséquent avoir une approche a minima méthodologique (identification, classement, choix, traitement, etc.). Non, car aucune méthode particulière n'est exigée par la norme ISO 9001:2015.

On peut lire dans l'annexe A de la norme ISO 9001:2015 *« Clarifications concernant la nouvelle structure, la terminologie et les concepts »* et en particulier dans l'article A4 : *« Approche par les risques »*, le texte suivant :

« Bien que le paragraphe 6.1 spécifie que l'organisme doit planifier des actions face aux risques, il n'y a pas d'exigence concernant des méthodes formelles de management du risque ou un processus de management du risque documenté. Les organismes peuvent décider d'opter ou non pour une méthodologie de management du risque plus étendue que ne l'exige la présente Norme internationale, par exemple par l'application d'autres lignes directrices ou normes. ». En ce qui concerne l'approche générale de management de risques, on trouve toujours les étapes citées ci-dessus, à savoir l'identification des risques, le classement, le choix des risques jugés majeurs et le traitement de ces risques majeurs. Il est d'usage d'utiliser des outils ou des méthodes dans certaines de ces étapes. Par exemple, le remue-méninge pour établir la liste la plus exhaustive des sources potentielles de risques. Par exemple, le couple Occurrence/Gravité (tiré des outils AMDEC, Analyse des Modes de Défaillances, de leurs Effets et de leurs Criticité) pour évaluer le niveau des risques et les classer par ordre d'importance. Mais cet outil n'est pas obligatoire. Il est tout à fait possible par exemple qu'un groupe de travail évalue des niveaux de risques de manière intuitive. Le consensus faisant loi dans ce cas.



5

Pour gérer les risques, laquelle de l'approche transversale ou par processus est préférable ?

L'approche par processus est de loin préférable. D'abord, c'est une exigence du référentiel ISO 9001:2015 mais c'est aussi une recommandation de la norme ISO 31000 sur le management des risques. Mais au-delà de ces raisons, la logique commande l'approche processus.

On a tendance à vouloir parfois affecter la responsabilité du traitement des risques à la composante (services ou processus) qui en est la cause. D'autre part, certains facteurs de risques peuvent impacter plusieurs processus et pour ces raisons, d'aucuns pensent qu'il faut une approche transversale. Par exemple confier aux RH les risques qui concernent les compétences ou les connaissances des personnels. Or, il faut se rappeler que la notion de risque est liée à celle de résultats. Il est exigé que chaque processus détermine et planifie les résultats attendus du travail de ses ressources. Les pilotes sont par conséquent responsables de gérer leurs processus en vue d'obtenir les résultats en question. Ils doivent donc identifier et évaluer les risques que ces résultats ne soient pas atteints et s'en occuper. Cela ne veut pas dire qu'ils doivent les traiter eux-mêmes car les causes de risques sont souvent exogènes. Leur responsabilité consiste à traiter ces risques en collaboration avec les responsables des causes exogènes et, si on ne peut agir sur ces causes, tenter d'en réduire les impacts ou les conséquences. Une approche transversale ne résoudra pas le problème du travail collectif de traitement des risques qui est incontournable en raison de la multiplicité des sources de risques et de la diversité de leurs origines.

6

L'approche par les risques exigée par la norme ISO 9001 doit-elle tenir compte des principes de la norme ISO 31000 sur le management des risques et, si oui, lesquels ?

La norme 9001 est constituée d'un ensemble d'exigences à satisfaire alors que la norme ISO 31000 est un guide proposant un concept et des principes. Cette dernière permet de comprendre ce concept et de le mettre en place dans un management de la qualité avec logique et bon sens.

Lors de la publication de la version 2015 de la norme ISO 9001, nous avions déjà été aidés par la publication concomitante du référentiel ISO 9000 sur les principes du management de la qualité et sur le vocabulaire. Par exemple, ce texte explique que les organismes sont confrontés à des défis nouveaux (évolution rapide du contexte, connaissances prises en compte comme une richesse, etc.) et que, de ce fait, le management de la qualité n'est plus celui du siècle passé (une qualité essentiellement basée sur un système documentaire) mais une nouvelle qualité basée sur des valeurs générant des comportements et des attitudes. La norme ISO 31000 nous propose, par exemple, dans son introduction quelques intérêts à adopter un management des risques. Elle cite entre autres que le management des risques :

- *« contribue à l'atteinte des objectifs, encourage l'innovation et améliore la performance »*
- *« améliore la prise de décisions à tous les niveaux »*

Le premier intérêt cité nous fait supposer que le management des risques est intimement lié à la notion de résultats et non pas à celle exclusive de « dangers ». Il élève la probabilité d'atteindre des objectifs escomptés et permet une plus grande optimisation des ressources.

Le deuxième intérêt renforce le premier : les décisions prises pour réduire les écarts constatés entre les résultats attendus et les résultats prévus seront plus fiables, ainsi que la planification si on prend en compte les risques de ne pas atteindre les résultats escomptés.

Dans les principes proprement dits que l'on découvre dans l'article 4, le texte nous explique, entre autres, que : « Le management du risque est intégré à toutes les activités de l'organisme, y compris la prise de décisions ».

Autrement dit, l'approche par les risques doit se faire dans chacun des processus d'un organisme et non de manière globale. Ce principe est repris dans la norme ISO 9001 à l'article 4.4 « Système de management de la qualité et ses processus » dans lequel on nous explique que chaque processus doit prendre en compte les risques et les opportunités qui le concernent.

7

Comment identifier et gérer les risques au niveau du management ?

Il faut travailler sur les réponses à apporter aux articles 4.1 et 4.2 de la norme ISO 9001:2015. Une non-compréhension des enjeux internes et externes ainsi qu'une non-écoute des parties intéressées constituent deux types de risques majeurs pour les organismes.

Dans la cartographie des processus, celui qui concerne le management de l'organisme est confronté à deux types de risques qui sont évoqués dans les deux articles cités plus haut. Mais auparavant, il faut se rappeler que l'approche « risques » telle qu'exigée par le référentiel ISO 9001 ne nécessite ni une identification ni surtout une gestion de tous les risques. L'esprit dans lequel il faut répondre à cette exigence est d'utiliser cette approche pour faire porter ses efforts d'amélioration là où cela donnera le plus d'effets. Un risque, comme le définit la norme ISO 9000, est un effet de l'incertitude, c'est-à-dire un écart positif ou négatif par rapport à une attente, par exemple, de résultats. Une direction doit proposer une vision à cinq ou dix ans qui s'exprimera, entre autres, en termes de résultats à atteindre. Les risques de ne pas atteindre les résultats en question sont déjà de deux natures. Le premier est de ne pas prendre en compte les enjeux internes et externes, c'est-à-dire les facteurs politiques, environnementaux, technologiques, etc. pour l'externe et les compétences existantes, la typologie des métiers exercés, etc. pour l'interne. Le second est de ne pas prendre en compte les attentes et les besoins des parties intéressées.

Identifier ces enjeux, les hiérarchiser, puis répondre à un ou deux choisis parmi les plus importants permet à la fois de satisfaire aux exigences de l'article 4.1 de la norme ISO 9001:2015 (« Compréhension de l'organisme et de son contexte ») et à la nécessité de mettre en place une approche « risques ». Il conviendra de procéder de la même manière en ce qui concerne l'écoute des parties intéressées. Identifier les parties intéressées, les hiérarchiser et ensuite en écouter une ou deux choisies parmi les plus influentes permet à la fois de satisfaire aux exigences de l'article 4.2 de la norme (« Compréhension des besoins et des attentes des parties intéressées ») et complète les dispositions prises pour mettre en œuvre une approche risques. Le référentiel ISO 9001 n'oblige aucunement à traiter un nombre déterminé de risques.

CHAPITRE 2

EVITER LES CHAUSSE-TRAPPES

8

Comment cadrer une réflexion sur les risques et éviter la production d'inventaires de risques incohérents ?

Il faut partir de la définition d'un risque : « Effet de l'incertitude sur les objectifs (ou les résultats) ». Si l'on commence par identifier les résultats attendus des activités d'un processus, alors l'inventaire sera cohérent.

Le premier travail à effectuer dans une analyse de risques relative à un processus particulier est de se poser la question des résultats attendus. Ces résultats seront exprimés de manière concrète en termes de quantités, de qualité, de délais, de coûts, de santé et sécurité au travail, de préservation de l'environnement, etc., qui constituent autant d'indicateurs de résultats à gérer sur le tableau de bord du processus en question. La liste des risques à inventorier sera alors constituée d'événements qui peuvent avoir une incidence négative sur les résultats énoncés en début d'analyse. Cela donne une première limite à la réflexion. Afin de cadrer encore un peu plus l'exercice, un second paramètre sera pris en compte, il s'agit de l'échéance des résultats. En effet, dans les processus de réalisation et de support, les résultats sont exprimés, en règle générale, à l'horizon d'une année maximum avec, très souvent, des échéances intermédiaires échelonnées à la semaine ou au mois. Il faudra donc prendre en compte les événements qui peuvent se produire dans ce laps de temps d'une année. Cela limite le nombre de risques. La plupart du temps, on en dénombre une douzaine au maximum. En ce qui concerne les processus de management, la liste des risques est souvent plus longue car l'échéance des résultats exprimés est assez lointaine (trois ans, cinq ans et parfois plus). C'est pour cette raison qu'il faut utiliser des outils d'aide à l'inventaire comme PESTEL par exemple, lequel permet de passer en revue des sources de risques stratégiques et éviter d'oublier quelques événements majeurs générateurs de risques. PESTEL est l'acronyme des mots Politique, Economique, Social, Technologique, Environnemental, Légal.

9

Faut-il inclure dans « l'approche par les risques » les risques que l'on n'a pas prévus ?

Non puisque par définition, un risque imprévu ne peut être identifié par avance. Cette question, qui peut sembler assez illogique voire même un peu idiote, ne l'est pas du tout. En effet, il est de la responsabilité d'un manager de s'interroger sur la performance de son approche des risques.

Le management des risques n'est pas une science exacte, tout le monde le sait. Et le plus grand risque de cette approche est justement d'oublier de prendre en compte un risque qui peut s'avérer funeste pour une organisation. La première étape d'un management des risques consiste à faire un inventaire de tous les événements, dangers ou situations à risques. Les outils qui sont utilisés en ce sens ne garantissent absolument pas le fait d'en oublier un. Chacun fait appel à sa mémoire, à des informations récoltées en interne ou en externe, mais une liste ne peut jamais être exhaustive. Cela se saurait car, dans ce cas, il n'y aurait plus aucun accident de travail, ni de dépôt de bilan, ni de catastrophe, ni de problème avec les clients, etc. Il existe donc par définition une probabilité plus ou moins grande qu'un événement dommageable non prévu puisse se produire. Dans ce cas, il est possible d'anticiper ce genre de situations et de mettre en place des systèmes de gestion de crise. Il existe des méthodes éprouvées en ce sens qui consistent à identifier un certain nombre de dispositions à actionner en cas de danger non prévu. Cela part de structures qui surveillent l'environnement à la recherche de signaux faibles annonciateurs de problèmes, jusqu'à la constitution de cellules de crise formées et organisées pour réagir très vite en cas de péril imminent, etc. On peut aussi, et c'est une obligation pour certains établissements publics comme, par exemple les hôpitaux ou les écoles, prévoir des dispositions qui permettent de ne pas interrompre une activité vitale pour un pays ou une communauté. Cela se nomme des PCA ou Plans de Continuité d'activité.

10

Pour le management des risques, faut-il un mode unique d'évaluation pour tous les processus ?

Non, ce n'est pas une obligation ni une logique standard. Les modes d'évaluation peuvent dépendre de la nature des activités et des conséquences envisageables.

Il ne faut pas oublier que les référentiels ISO 9001:2015 et ISO/DIS 31000 nous demandent de mettre en place un management des risques dans chaque processus. Or ceux-ci peuvent s'appliquer à des métiers différents. Dans tel processus on effectuera des achats, dans tel autre de la production et dans un troisième, de la conception et du développement de produits. D'autre part, les processus de management travaillent pour le futur et les risques qui les concernent ont un caractère stratégique qui nécessite une pratique d'évaluation particulière.

Dans les processus de réalisation et de support, les risques qu'il faut envisager sont ceux qui peuvent obérer les résultats attendus de leurs activités. Ceux-ci sont des résultats opérationnels à court terme et, en règle générale, les risques sont générés par des événements déjà constatés et qui peuvent se reproduire. On utilisera alors des critères d'évaluation tels que l'occurrence ou la fréquence (la probabilité de réapparition) et la gravité. On pourra par exemple utiliser des notations sur quatre niveaux. Pour l'occurrence, on notera 1 si l'événement redouté ne s'est jamais produit, 2 s'il est rare, 3 s'il a été déjà constaté quelquefois et 4 souvent. En ce qui concerne les risques à caractère stratégique qui peuvent obérer les résultats à long terme, les événements générateurs de problème peuvent ne s'être jamais produits. On travaillera alors non pas sur la fréquence (l'occurrence), mais sur la vraisemblance (qui est d'ailleurs le terme consacré dans le référentiel ISO/DIS 31000).

En ce qui concerne la gravité de ce type de risques, au lieu d'utiliser une échelle de 1 à 4 comme pour l'occurrence des risques relatifs aux processus de réalisation et de support, on pourra utiliser alors une échelle dérivée du diagramme de Farmer (ingénieur nucléaire britannique) et travailler avec quatre niveaux numérotés 1 (pas grave), 10 (assez grave), 50 (grave) et 100 (très grave). Ce système de notation permet de faciliter la prise en compte dans le classement final des risques dont la vraisemblance est faible mais dont la gravité des conséquences est très élevée.

Et pour terminer, j'ajouterai que chaque niveau de gravité des conséquences dans les processus de réalisation et de support peut être expliqué avec une description des effets spécifiques dans chaque processus. Dans celui-ci, la gravité 3 sera induite par le paiement d'indemnités et dans celui-là, ce niveau 3 sera généré par le retour de produits non conformes.

11

Une source de problème prévisible peut-elle être considérée comme un risque ?

Dans la pratique oui, bien que la définition du mot « risque » soit « effet de l'incertitude sur un objectif ». En théorie, un risque est un événement comportant une part d'incertitude dans sa probabilité d'apparition.

On entend également ici et là qu'un événement qui s'est déjà produit ne peut être classé en tant que risque. Ce raisonnement n'est pas très juste car le risque concerne alors la probabilité de réapparition d'un tel événement ou d'un événement semblable à celui qui s'est déjà produit. Cette probabilité est empreinte d'incertitude. Pour en revenir à l'exemple de la pyramide des âges, dans ce cas effectivement, il n'y a pas d'incertitude mais c'est une source de problèmes à envisager dans un avenir plus ou moins lointain. Cela génère donc un risque pour les résultats à long terme d'une entreprise si l'on ne s'en occupe pas. On pourra alors considérer l'incertitude comme une possibilité de ne pas retrouver les compétences qui partiront avec le départ des personnels en âge de prendre leur retraite. Mais peu importe si le problème ne correspond pas à un risque dans sa définition. Lorsque les personnes concernées partiront, si l'on ne s'est pas occupé de ce sujet, les résultats envisagés peuvent ne pas être atteints. De ce fait, il est inutile de procéder à deux réflexions différentes, une sur les vrais risques et l'autre sur les problèmes (non classés en risques). Si la thématique de la réflexion consiste à se demander quels sont les événements qui peuvent avoir une incidence négative sur les résultats espérés, alors on prendra en compte toutes les sources d'ennuis envisageables.

12 La criticité d'un risque peut-elle toujours être évaluée avec le produit « Probabilité » et « Gravité » ?

Non, ce produit (probabilité x gravité) est un usage qui nous vient des méthodes utilisées en production et qui parfois d'ailleurs s'accompagne d'un troisième facteur comme la « probabilité de non-détection du risque » comme dans les outils AMDEC (Analyse des modes de défaillance, de leurs effets et de leurs criticités).

Aujourd'hui et notamment avec la version 2015 de la norme ISO 9001, la prise en compte des risques et opportunités est devenue une nécessité, voire une obligation, dans tous les processus. Or si les risques liés aux non-conformités peuvent toujours être évalués avec ce couple « Occurrence » et « Gravité », il en est d'autres pour lesquels cette approche n'a pas de sens. On peut évoquer les risques à caractère stratégique, par exemple. L'utilisation de la « probabilité » s'appuie sur une connaissance du passé et de la survenue d'événements de même nature. Lorsqu'un groupe de travail s'interroge à propos de la probabilité d'apparition de traces de copeaux sur une pièce usinée, il se demande si cette situation est déjà arrivée dans le passé. Si la réponse est « Non jamais », la probabilité d'apparition sera très faible et, par exemple, notée 1. Si la réponse est « Rarement » ou « Quelquefois », la probabilité de réapparition est plus forte et sera notée 2 et 3. Si la réponse est « Souvent », alors la probabilité de récurrence sera très élevée et en conséquence notée 4. En matière de stratégie, si un risque est lié à une législation qui peut interdire l'emploi d'un matériau, ce critère n'est pas utilisable car une telle loi n'a jamais été votée dans le passé. Pour des risques liés à la continuité de fonctionnement, celui d'une inondation, par exemple, ne peut être évalué sur la base de statistiques passées (c'est arrivé une seule fois en 1908 avec la crue du siècle).

On parlera alors de vraisemblance d'apparition du risque. Par exemple si l'organisme est situé en montagne, la vraisemblance d'une crue est nulle. En revanche, si une rivière passe à proximité, la vraisemblance est plus élevée même si la catastrophe ne s'est jamais produite auparavant. C'est d'ailleurs ce terme que la norme ISO 31000 « Management du risque – Principes et lignes directrices » utilise dans son vocabulaire.

13

Quel niveau de risques peut être considéré comme acceptable dans une approche par les risques ?

Il n'y en a pas. Bien entendu, le niveau d'acceptabilité qui est déterminé au cas par cas dans les entreprises dépend du type de management concerné. Dans le cas d'un management de la santé et sécurité au travail, le zéro risque est l'objectif recherché. Dans le cas d'un management de la qualité, la situation est tout autre.

En effet, le mode de fonctionnement d'un entrepreneur est la prise de risques et, en matière de management de la qualité, cette notion est omniprésente. Même si l'inventaire des risques et leur analyse sont parfois intuitifs et non formels, ils existent toujours. Un entrepreneur pèse, comme on dit, le pour et le contre avant de prendre une décision.

D'ailleurs dans l'article 6.1 intitulé « *Actions à mettre en œuvre face aux risques et opportunités* », on peut lire la note 1 qui rappelle que : ***« Les options face aux risques peuvent comprendre : éviter le risque, prendre le risque afin de saisir une opportunité, éliminer la source du risque, modifier la probabilité d'apparition ou les conséquences, partager le risque ou maintenir le risque sur la base d'une décision éclairée. »***

On apprend donc qu'un risque peut être pris en toute conscience pour saisir une opportunité. D'ailleurs il eût été plus logique d'intituler cette approche « par les opportunités et les risques » plutôt que l'inverse car, dans une entreprise, les responsables et les managers sont toujours à la recherche d'opportunités qui leur permettront de se développer avec, à la clé, des risques plus ou moins importants. Récemment, le patron d'une entreprise de découpage a terminé la mise au point d'une membrane en aluminium qui lui a demandé deux ans et demi de développement. Ce produit est destiné à équiper des enceintes Hifi de très haute gamme. Il n'a pas procédé à une analyse précise de risques avant de s'engager dans cette aventure.

Il a jugé que c'était (peut-être) une belle opportunité de progresser dans sa technique de découpe et d'emboutissage et de faire croître ainsi son entreprise. Le pari est aujourd'hui réussi mais comment dans ce cas, juger d'un niveau de risque inacceptable ? Cette évaluation ne peut être qu'informelle. Il n'était pas capable de savoir si le défi technologique qu'il avait accepté était réalisable. Il ne pouvait évaluer d'aucune façon un niveau de risque quelconque. Or cette décision était un acte majeur pour l'entreprise. C'est pour cette raison qu'il faut toujours conserver en mémoire que l'approche par les risques et opportunités ne doit en aucun cas constituer un frein pour le développement d'un organisme.

14

L'analyse des risques dans un processus peut-elle se limiter à ceux relatifs aux interactions ?

Non car il existe au moins deux typologies de risques dans un processus et on pourrait même dire qu'il en existe parfois une troisième catégorie. Les risques liés aux interactions sont globalement les risques de produire des données de sortie non conformes.

Effectivement, la probabilité et la gravité de produire des données de sortie non conformes sont une première catégorie de risques et se situent dans les interactions puisqu'une donnée de sortie non conforme sera livrée au client interne ou externe. De ce fait, elle sera attachée à l'interaction entre le processus qui produit et le processus qui reçoit. Ce type de risque s'évalue à partir de l'occurrence et de la gravité de chaque non-conformité identifiée.

Il y a ensuite le risque que le processus ne produise pas le résultat attendu. L'utilisation du cycle PDCA dans chaque processus conduit les pilotes à identifier les résultats attendus (planifiés) du travail de ses ressources internes. Ces objectifs opérationnels sont généralement discutés entre les directions et les pilotes et ces derniers doivent tout naturellement réfléchir à la survenue d'événements qui seraient susceptibles d'obérer les résultats en question. Il faut donc les identifier et les traiter (pour les plus importants en tout cas). Il peut y avoir par exemple des problèmes d'absentéisme ou de rupture de stock pour n'en citer que deux.

Et puis enfin, il est possible que certains des processus d'un organisme soient affectés d'objectifs particuliers qui découlent des « objectifs qualité » décidés par la direction. Ces objectifs qualité, lorsqu'ils sont déployés dans l'organisme, se concrétisent par des projets ou des actions à mettre en place afin que les processus concernés participent à l'atteinte des objectifs qualité globaux cités ci-dessus. Là encore, il peut y avoir des risques que les actions souhaitées ne soient pas menées à bien en ce qui concerne les coûts, les résultats ou les échéances. Ces risques doivent donc eux aussi être identifiés et traités pour les plus importants.

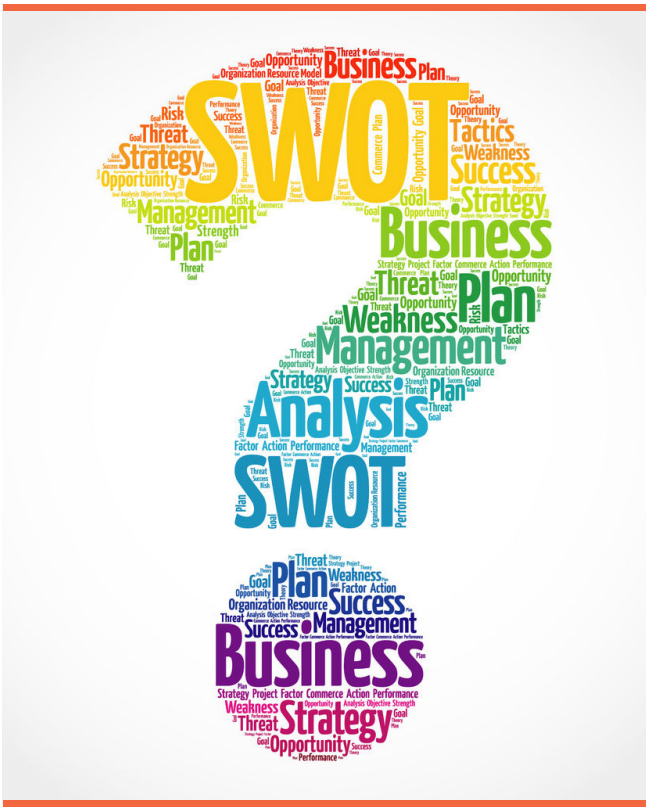
15

Peut-on utiliser les matrices SWOT pour répondre à l'approche par les risques de l'ISO 9001:2015 ?

Oui bien entendu, mais cet outil n'est pas tout à fait adapté à l'ISO 9001 et peut compliquer la compréhension de ceux qui sont chargés de mettre en place et d'expliquer l'approche par les risques.

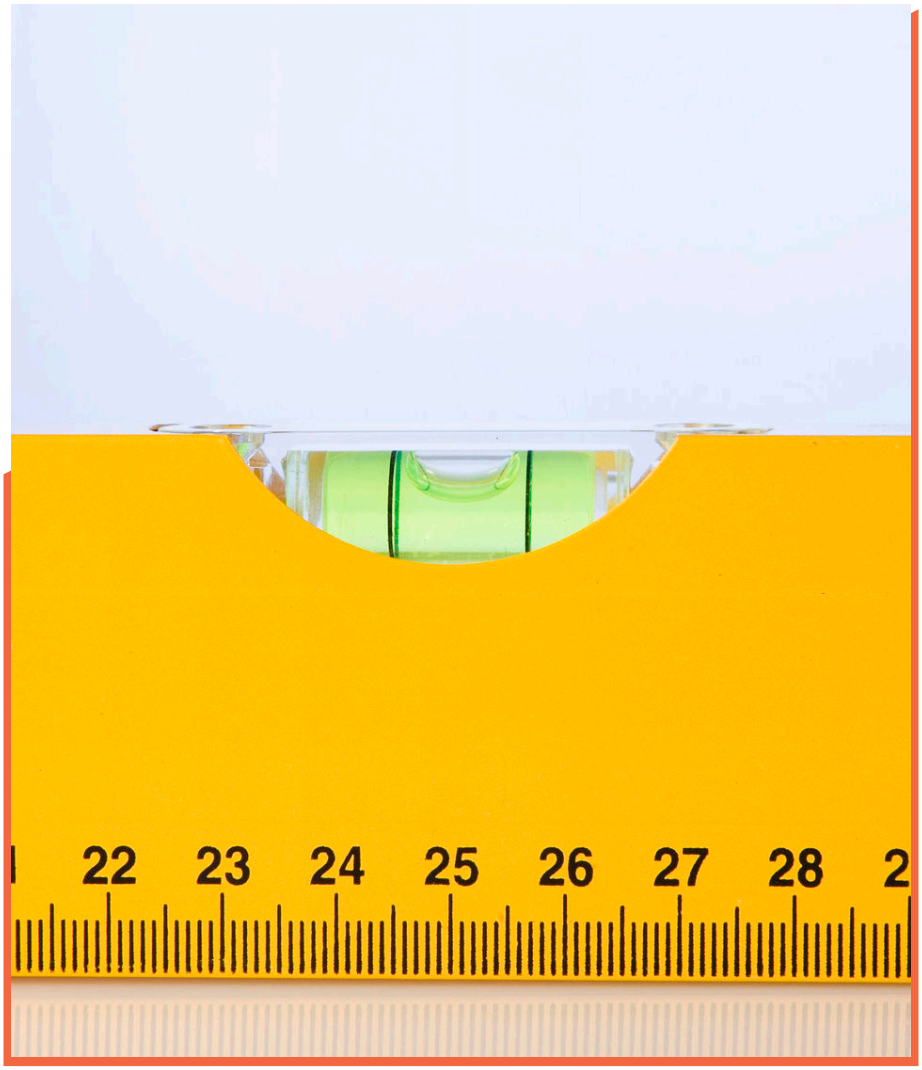
Tout d'abord, le problème réside dans le nombre de critères à prendre en compte. L'analyse SWOT utilise les notions de « forces et faiblesses et de menaces et d'opportunités ». La norme ISO 9001 parle quant à elle de « risques et opportunités ». Il vaut mieux se cantonner à deux notions plutôt qu'à quatre si l'on n'est pas familiarisé avec le SWOT. Effectivement, on aurait pu s'attendre à ce que le référentiel ISO 9001 utilise aussi la notion de « danger » qui est un préalable à une évaluation des risques présentés par le danger en question. Cela correspondrait à la notion de menaces évoquée dans le SWOT. Ensuite, il est habituel de considérer que les forces et faiblesse concernent des éléments internes à l'entreprise et que les menaces et opportunités concernent des éléments externes. Bref, c'est un peu plus compliqué d'utiliser cette matrice que de procéder à une identification plus basique des risques et des opportunités. La matrice SWOT présente un inconvénient plus important dans une utilisation éventuelle pour la mise en place d'un système de management de la qualité. C'est un outil d'analyse stratégique et, si elle peut être utilisée avec bonheur dans les processus de management pour lesquels les enjeux externes et internes (Cf. § 4.1 « Contexte de l'organisme ») constituent autant de menaces et d'opportunités, en revanche l'analyse de risques dans les processus de support et de réalisation ne présente en règle générale pas de caractère stratégique ni prospectif. Les risques en question sont plutôt des risques de type « opérationnels » c'est-à-dire pour des objectifs à atteindre à court terme (semaine, mois année).

Il est par conséquent plus simple de commencer par identifier, si ce n'est déjà fait, les résultats attendus du travail des ressources d'un processus, puis ensuite de se poser la question de l'identification des risques qui peuvent avoir un impact négatif sur lesdits résultats.



CHAPITRE 3

MANAGER AU PLUS JUSTE



16

Quel est le rôle d'un risk-manager dans un organisme ?

Il n'est certainement pas de s'occuper tout seul du management des risques. Son rôle consiste essentiellement à déployer l'approche par les risques et à l'animer.

Le rôle d'un risk manager, comme celui d'un responsable qualité d'ailleurs pour sa spécialité, est de s'assurer qu'une culture du risque est déployée dans toute l'organisation et sur tous les postes de travail. Même s'il est formé aux techniques de management des risques et à diverses méthodologies et outils (comme le SWOT par exemple ou PESTEL), il ne possède pas les compétences pour identifier les occurrences lorsque l'on s'appuie sur le passé pour le faire (il n'a pas la mémoire de l'histoire de toutes les activités et de tous les processus). De plus, il ne possède pas non plus la connaissance qui permette d'identifier les impacts potentiels d'un événement (les dommages qui peuvent être causés par la survenue d'un évènement) car il ne connaît pas les tenants et les aboutissants du fonctionnement de tous les processus de son organisme. Il peut bien entendu animer des réunions de groupes de travail composés d'individus qui, eux, disposent de cette connaissance mais il sera plus efficace s'il transmet les outils à la hiérarchie opérationnelle afin qu'elle puisse elle-même animer et manager les risques qui concernent son secteur d'activité. Il en va de même pour les risques relatifs à une non-conformité réglementaire. Même s'il est le spécialiste de la réglementation, il va de soi que chaque individu doit connaître les contraintes réglementaires concernant ses propres activités et de ce fait connaître les risques qui en découlent. Cette connaissance de la réglementation doit, elle aussi, être déployée dans toute l'organisation.

17

Faut-il prendre des dispositions pour tous les risques évalués comme importants ?

Non car il ne faut pas oublier que l'engagement dans une démarche qualité vise à fournir des prestations régulièrement conformes et à améliorer en permanence la satisfaction des clients. Il s'agit donc de mettre en œuvre une dynamique d'amélioration efficace et l'approche « risques » est un outil en ce sens.

Dans un contexte difficile et concurrentiel pour certains organismes, il faut montrer de la performance à tous les niveaux et l'amélioration continue est un facteur clé de succès dans de très nombreux cas. Dans les versions précédentes, l'amélioration était générée par des actions correctives suite à des constats de non-conformités et par des actions préventives suite à des analyses de risque de non-conformités. Elle était engendrée également par des actions issues de la surveillance des processus (en cas d'écart entre résultats planifiés et résultats réalisés) et par des constats en provenance d'audits internes ou d'enquêtes faites auprès des clients. Dans tous les cas, l'amélioration était une amélioration essentiellement basée sur des constats de dysfonctionnement ou de fonctionnements manquant d'efficacité. Il n'était pas certain que des thématiques essentielles soient le sujet d'action d'amélioration.

L'approche « risques » est un outil qui permet d'identifier des situations pour lesquelles il n'y a jamais eu de problème mais qui peuvent se révéler catastrophiques le cas échéant pour les organismes. Dans la version précédente, il y avait obligation d'action préventive mais il n'y avait pas d'exigence de disposer d'une méthodologie d'identification des risques et, dans les faits, la plupart des organismes ne montraient pas beaucoup d'action en ce sens.

L'approche « risques » permet d'explorer tous les domaines qui peuvent présenter des risques (stratégie, opérations) et de sélectionner ceux qui doivent faire l'objet de dispositions pour les supprimer, les réduire, les contourner ou s'assurer contre les conséquences possibles. Les organismes vivent déjà avec de nombreux risques qui peuvent nuire à leur développement et à leur pérennité et il n'est pas question qu'elles se prémunissent contre tous ces risques potentiels et qu'elles deviennent du jour au lendemain des zones à risque zéro. Il serait utopique d'envisager de telles actions. Cela demanderait de trop grandes ressources qu'elles ne peuvent distraire des activités quotidiennes. Ce qui est demandé avec logique et bon sens, c'est qu'elles consacrent régulièrement un peu de moyens pour travailler sur quelques risques majeurs et ainsi améliorer leur fonctionnement sur des thématiques essentielles.

18

L'approche risque de l'ISO 9001 rend-elle indispensable un processus de management des risques ?

Non, il n'y a aucune exigence de « management » des risques mais une exigence d'avoir une « approche » par les risques, c'est-à-dire de prendre en compte les risques et opportunités. Et par conséquent, il n'y a pas de nécessité de mettre en place un processus de management des risques.

Le risque le plus important en l'occurrence est de construire une usine à gaz pour répondre à cette approche par les risques. La norme ISO 9000 relative aux principes et au vocabulaire du management de la qualité peut nous aider à mettre en place une approche par les risques logique et de bon sens et dans un premier temps « minimaliste ». Tous les risques ne sont pas égaux et il serait ridicule de passer d'une situation où l'on ne se préoccupe pas des risques (de manière structurée et organisée) à une situation où l'on voudrait gérer tous les risques. Ce qui est donc important est de mettre en œuvre cette approche afin que cela permette une amélioration des performances régulière des organismes. La norme ISO 9000 explique, dans son article § 3.7.9 « Risque », qu'un risque est l'effet de l'incertitude. Une note précise que cela peut être un écart positif ou négatif lié à une attente. Un avant-projet de ce référentiel expliquait, à mon avis d'une manière plus précise, que le risque était l'effet de l'incertitude sur un résultat. Si l'on se cantonne à cette définition, et rien ne nous en empêche, il suffit alors de pratiquer une approche par les risques chaque fois que l'on attend un résultat d'une activité. Or dans un organisme, tous les résultats attendus ne sont pas de la même importance. Il conviendra alors de restreindre l'approche par les risques aux résultats majeurs tels que les résultats économiques (influencés par la démarche qualité), aux résultats attendus des activités de chaque processus (résultats économiques mais aussi relatifs à la qualité, c'est-à-dire de ce qui est attendu par les clients).

Par exemple ce que l'on attend d'un processus de management, ce sont des résultats à long terme (chiffres d'affaires, budgets, dépenses, marges, amélioration des services et des produits vendus ou fournis, etc.) et ce processus nécessitera d'examiner les facteurs de risques qui peuvent obérer les résultats en question. Dans les autres processus, on attend des résultats à plus court terme sur les mêmes sujets que ceux évoqués quelques lignes plus haut et les pilotes s'interrogeront sur les facteurs de risques qui peuvent obérer les résultats attendus au niveau de chaque processus de l'organisme

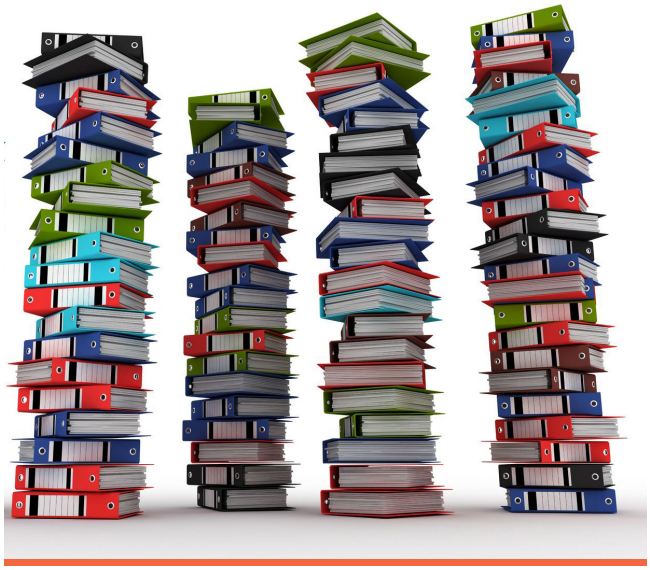
19 Comment démontrer que l'on a mis en œuvre une approche risques ?

En rédigeant et en conservant des comptes rendus de réunions tenus sur cette thématique. Les comptes rendus de réunions constituent en effet des informations documentées en sens des exigences de la norme ISO 9001 :2015.

Les exigences concernant l'approche « risques » sont montrées essentiellement dans l'article 4.4 de la norme ISO 9001:2015 qui s'intitule : *« Système de management de la qualité et ses processus »*. Le texte dit en substance à l'alinéa f) que chaque processus doit : *« Prendre en compte les risques et opportunités tels que déterminés conformément aux exigences de 6.1 ; »*.

Cela concerne tous les processus de l'organisme c'est-à-dire ceux qui ont été déterminés comme étant nécessaires au système de management de la qualité. Cela inclut par conséquent les processus de management, ceux de réalisation et les supports. Il faut que chaque processus procède à un inventaire des risques en regard des résultats à atteindre. Pour les processus de management ces résultats sont ceux attendus par l'organisme et exprimés par exemple en termes de chiffres d'affaires, de projets, etc. Pour les autres processus, il s'agit d'identifier dans le même esprit les risques que le processus en question n'atteigne pas les résultats attendus et qu'il a planifiés. Chaque processus provoque une réunion avec les personnels concernés. Par exemple les membres du Codir pour le management, le pilote et quelques acteurs du processus pour les autres. Au cours de cette réunion, les participants identifient les risques qui peuvent impacter les résultats espérés produits par le processus dans lequel ils travaillent, les classent par ordre d'importance et décident de traiter un ou deux sélectionnés parmi les plus impactant. Il suffit alors qu'un compte rendu soit formalisé en décrivant les inventaires effectués, les analyses, les choix et les actions qui ont été décidées et qui seront engagées. Pour ces dernières, elles peuvent être renseignées sur un tableau spécialement destiné à la gestion des actions d'amélioration de chaque processus. Il conviendra de faire cette opération régulièrement (par exemple une fois par an) car les causes de risques peuvent changer ou bien encore de nouveaux risques peuvent apparaître.

Le compte rendu précisera si les risques que l'on a identifiés peuvent devenir des opportunités pour améliorer les résultats espérés et, dans l'affirmative, comment ces opportunités seront traitées (par exemple sous forme de projets spécifiques).



20

Comment un auditeur peut-il évaluer la qualité de l'analyse des risques effectuée par l'entreprise ?

Il n'est pas possible d'évaluer la qualité de l'analyse de risques mais on peut s'assurer qu'une analyse a été réalisée et qu'elle couvre le périmètre certifié et les activités concernées.

L'approche « risques » est un sujet éminemment complexe et elle peut être aussi bien sous dimensionnée que surdimensionnée. Un auditeur ne peut pas exiger par exemple que cette approche aille au-delà des exigences du référentiel ISO 9001, c'est-à-dire qu'elle aborde d'autres champs de risques que ceux relatifs au management de la qualité. Il n'y a pas d'exigence d'identifier des dangers concernant les impacts environnementaux ou liés à la santé et sécurité au travail. Certains organismes peuvent, si cela leur parait intéressant conduire une analyse de risque sur plusieurs champs de manière consécutive mais l'auditeur s'attachera à ne regarder que ceux relatifs à la qualité. Il n'y a pas non plus d'obligation à utiliser des outils pour identifier les risques et opportunités. L'inventaire des dangers peut se faire de manière intuitive ainsi que l'évaluation des risques. Ce qui est important c'est qu'il existe une méthodologie, même rudimentaire de manière à ce que cette approche soit possible et récurrente pour tous types d'organismes.

Il est possible d'aborder l'audit de l'approche « risques » de deux manières différentes soit à travers une analyse exhaustive des différents articles de la norme (par exemple les risques relatifs à la compréhension du contexte ou bien encore aux parties intéressées ont-ils été identifiés et valorisés, etc. ?) soit à travers l'existence d'une analyse des risques dans chacun des processus de l'organisme.

On pourra ainsi s'assurer dans ce second cas, que les processus de management ont conduit une analyse en considérant les risques à caractère stratégique et que les autres processus ont conduit une analyse en considérant les risques à caractère opérationnels. Par exemple que les risques de produire des données de sortie non conformes ont été identifiés et évalués.

Il n'est pas possible de s'assurer que tous les risques ont été identifiés et valorisés à leur juste niveau. Une approche risque est forcément empreinte d'incertitude. Ce qui est important c'est de s'assurer que la quasi-totalité des activités ont été analysées, et que des dispositions ont été prises pour répondre conséquences possibles de ces évaluations.

Parcours Croisés est une plateforme qui vous est entièrement dédiée.

Vous y trouverez tout pour enrichir votre réseau, profiter d'avis d'experts, suivre les tendances et développer vos compétences.

Suivre les tendances

Des groupes d'échanges pour débattre des dernières initiatives qui feront les solutions de demain.

Développer vos compétences

Un lieu où piocher des outils et pratiques pour progresser dans votre fonction.

AFNOR parcours croisés

www.parcourscroises.com

Enrichir votre réseau

Une plateforme pour faciliter les rencontres de qualité.

Profiter d'avis d'experts

Des outils et des points de vue pour décrypter l'actualité et élargir vos perspectives.

Un grand merci à

Yvon Mougin, auteur des questions/réponses reproduites ici et extraites de la rubrique « Question de la semaine » du site Bivi, bibliothèque virtuelle des responsables QSE

S1804101 • ADE- Studio DMK : Groupe AFNO • Copyright @ AFNOR.
Crédits photos : ©Getty images : Photick/Ale Ventura, Jeffrey Hamilton • ©AdobeStock : rostyle, Africa Studio, shersor • © Stocklib : coonlight, yganko, Marc Dietrich, belchonock, giuseppe porzani, El Roi, Giedrė Vaitekūnė, reddz, Sergiy Tryapitsyn, Ramona Geers, ravital, lightwise, dizanna, mearicon, oksix, Damir Bayburin, destinacigdem, Brian Jackson