JOAILLERIE : DE L’ACTIVITÉ AU RISQUE RÉSIDUEL

Méthode intégrée ISO 31000 + COSO pour identifier, prioriser, contrôler, mitiger et piloter les risques

Table des matières

Introduction — Une gestion des risques qui part de l’entreprise réelle

Chapitre 1 — Cadre de management des risques : ISO 31000 et COSO

Chapitre 2 — Définir objectifs, contexte, critères, appétence et tolérances

Chapitre 3 — Construire l’univers des activités de la société

Chapitre 4 — Construire l’univers des risques et la taxonomie sectorielle

Chapitre 5 — Exploiter les informations externes et internes pour identifier les risques

Chapitre 6 — Formuler les scénarios et évaluer le risque inhérent

Chapitre 7 — Matrice Impact × Vraisemblance et priorisation

Chapitre 8 — Construire l’univers des contrôles internes et des documents/preuves

Chapitre 9 — Évaluer le design et l’efficacité opérationnelle des contrôles

Chapitre 10 — Déterminer et visualiser le risque résiduel

Chapitre 11 — Traiter et mitiger les risques

Chapitre 12 — KRI, tendances, signaux émergents et mise à jour continue

Chapitre 13 — Reporting management, direction et conseil

Chapitre 14 — Cas fil rouge joaillerie : de l’activité au risque résiduel

Chapitre 15 — Gouvernance, Trois Lignes et cadence de revue

Fiche méthode A — Définir les critères et l’appétence

Fiche méthode B — Construire l’univers des activités

Fiche méthode C — Construire l’univers des risques

Fiche méthode D — Transformer un signal externe en risque

Fiche méthode E — Scorer et prioriser le risque inhérent

Fiche méthode F — Construire la bibliothèque de contrôles

Fiche méthode G — Tester design et efficacité opérationnelle

Fiche méthode H — Évaluer le risque résiduel

Fiche méthode I — Définir le traitement et la mitigation

Fiche méthode J — Construire les KRI et le reporting

Conclusion — De la cartographie à l’assurance décisionnelle

Plan d’action — Construire le dispositif en 30 jours

Glossaire

Sources et références

Méthode intégrée ISO 31000 + COSO pour identifier, prioriser, contrôler, mitiger et piloter les risques d’une maison de joaillerie

Version méthodologique approfondie - ASCALEA

Introduction — Une gestion des risques qui part de l’entreprise réelle

Une maison de joaillerie combine des actifs à forte valeur, des chaînes d’approvisionnement internationales, des contraintes de traçabilité, des enjeux de sécurité, des données clients, des canaux physiques et numériques, ainsi qu’une forte sensibilité de marque. Une cartographie de risques utile ne peut donc pas commencer par une liste générique. Elle doit partir des objectifs de l’entreprise et de son univers d’activités.

La démarche développée dans ce guide suit une logique continue : objectifs → activités → risques → informations externes et internes → risque inhérent → priorisation → contrôles → preuves → risque résiduel → traitement → KRI → reporting → revue.

ISO 31000:2018 fournit la colonne vertébrale du processus. COSO ERM 2017 relie le risque à la stratégie et à la performance. COSO Internal Control structure l’analyse des contrôles internes. IEC 31010:2019 complète le dispositif par des techniques d’appréciation du risque.

Les risques prioritaires illustrés dans ce guide sont des **candidats sectoriels**. Ils ne doivent pas être présentés comme les véritables top risques d’une entreprise donnée sans analyse de ses données internes, incidents, volumes, marchés, contrôles et appétence.

Chapitre 1 — Cadre de management des risques : ISO 31000 et COSO

Le premier choix méthodologique consiste à distinguer trois questions. ISO 31000 répond principalement à « comment organiser le processus de management du risque ? ». COSO ERM répond à « comment intégrer le risque dans la stratégie, les objectifs et la performance ? ». COSO Internal Control répond à « comment structurer et évaluer la maîtrise interne ? ». Ces cadres sont complémentaires, pas concurrents.

ISO 31000:2018 décrit un processus cyclique : définir le champ, le contexte et les critères ; identifier les risques ; les analyser ; les évaluer ; définir et mettre en œuvre un traitement ; communiquer, consulter, surveiller, revoir et documenter. Ce cycle doit être intégré aux décisions de l'entreprise.

COSO ERM 2017 ajoute une dimension stratégique : gouvernance et culture, stratégie et définition des objectifs, performance, revue et révision, information/communication/reporting. Pour une maison de joaillerie, cela signifie que le risque ne doit pas être séparé des choix de marchés, de collection, de sourcing, de canaux de vente, de financement du stock ou d'image de marque.

COSO Internal Control, rafraîchi en 2013, sert ensuite à analyser la couche de contrôle : environnement de contrôle, évaluation des risques, activités de contrôle, information/communication et monitoring.

IEC 31010:2019 n'est pas un quatrième cadre de gouvernance : il aide à choisir des techniques d'appréciation du risque selon la question à résoudre.

Cadre	Rôle principal	Utilisation dans ce livre
ISO 31000:2018	Processus de management du risque	Contexte → identification → analyse → évaluation → traitement → revue
COSO ERM 2017	Stratégie, objectifs, performance	Appétence, priorisation, gouvernance, reporting
COSO Internal Control	Maîtrise interne	Design, exécution, information, monitoring
IEC 31010:2019	Techniques d'appréciation	Matrice, scénarios, analyse causes, bow-tie lorsque pertinent

Erreur fréquente : citer « COSO 2019 » comme cadre ERM générique. La publication ERM de référence est celle de 2017. La publication COSO de 2019 sur le cyber est une application thématique du cadre ERM.

À retenir : ISO 31000 organise le cycle du risque, COSO ERM le relie aux choix de l'entreprise, COSO Internal Control structure la maîtrise.

Chapitre 2 — Définir objectifs, contexte, critères, appétence et tolérances

Le risque n’existe pas en soi : il existe par rapport à un objectif. Avant de chercher les risques, il faut donc rendre explicites les objectifs stratégiques et opérationnels : croissance, marge, disponibilité des produits, qualité, conformité, sécurité, réputation, liquidité, traçabilité et expérience client.

Le contexte externe comprend les marchés, les prix des métaux, les taux de change, les sanctions, les exigences sectorielles, les technologies, les attentes clients, la concurrence et les événements géopolitiques. Le contexte interne comprend la structure, les canaux, les produits, les fournisseurs, les systèmes, les ressources, les niveaux de stock, les politiques et la culture de contrôle.

Les critères de risque définissent comment l’entreprise apprécie l’impact et la vraisemblance. Ils doivent être écrits avant le scoring afin d’éviter de déplacer les seuils après coup.

L’appétence au risque exprime le niveau général que l’organisation est prête à accepter pour poursuivre ses objectifs. Les tolérances traduisent cette appétence en limites opérationnelles observables : variation de marge, exposition fournisseur, nombre d’accès sensibles, perte acceptable, délai de reprise, seuil d’écart inventaire, etc.

Objet	Question	Exemple joaillerie
Objectif	Que veut-on protéger / atteindre ?	Marge brute par collection
Critère d'impact	Quand l'impact devient-il majeur ?	Perte > seuil ou incident réputationnel
Appétence	Quel niveau global est acceptable ?	Faible pour fraude / sécurité
Tolérance	Quelle limite opérationnelle ?	Écart inventaire < 0,5% de la valeur
KRI	Quel signal montre une dérive ?	% de fournisseurs critiques sans alternative

À retenir : sans objectifs, critères et tolérances, la heat map devient un exercice de perception plutôt qu’un outil de décision.

Chapitre 3 — Construire l’univers des activités de la société

L’univers des activités est le référentiel commun qui évite les cartographies de risques déconnectées des opérations. Il décrit ce que l’entreprise fait, où elle le fait, avec quels systèmes, données, tiers et actifs.

La construction part généralement des chaînes de valeur puis descend jusqu’au niveau où le risque devient actionnable. Une granularité trop fine produit des centaines de lignes inutilisables ; une granularité trop large masque les propriétaires et les contrôles.

Niveau 1 : chaînes de valeur et grandes fonctions.

Niveau 2 : processus.

Niveau 3 : sous-processus / activité critique.

Niveau 4 : uniquement pour les zones à forte exposition ou forte complexité.

Domaine	Activités	Données / actifs clés
Création & design	collections, prototypes, dessins	IP, fichiers, lancements
Sourcing	métaux, pierres, fournisseurs	origine, coût, qualité
Fabrication	fonte, usinage, sertissage, polissage	matière, rendement, sécurité
Stock & sécurité	coffre, inventaire, mouvements	valeur, traçabilité
Vente	boutique, wholesale, e-commerce	client, paiement, remise
Finance	pricing, change, trésorerie, valorisation	marge, liquidité
IT & données	ERP, e-commerce, accès, sauvegardes	disponibilité, confidentialité
ESG / conformité	due diligence, sanctions, disclosure	accès marché, réputation

Méthode : pour chaque activité, documenter objectif, propriétaire, systèmes, tiers, entrées, sorties, documents internes, données et dépendances. Ce dossier devient ensuite le point d’ancrage des risques, contrôles et tests.

À retenir : une activité mal définie produit un risque mal attribué et un contrôle sans propriétaire.

Chapitre 4 — Construire l’univers des risques et la taxonomie sectorielle

L’univers des risques organise les expositions en familles cohérentes tout en conservant le lien avec les activités. Une famille telle que « fraude » ou « sourcing » n’est pas encore un risque : elle sert de taxonomie.

Un scénario de risque utile suit la logique : cause ou condition → événement redouté → conséquence sur un objectif.

Exemple : si une pierre de laboratoire est intégrée au stock naturel sans séparation, test ou attribut système, l’entreprise peut vendre un produit mal décrit, provoquant remboursement, perte de marge, non-conformité et atteinte à la confiance.

Famille	Scénarios candidats
Marché / financier	prix or, FX, marge, valorisation stock
Sourcing / tiers	sanctions, origine, dépendance fournisseur
Fraude / sécurité	vol, substitution, faux paiement, retours
Produit / qualité	composition, disclosure, rappel, défaut
Cyber / données	indisponibilité, accès, ransomware, fuite
ESG / réputation	controverse origine, droits humains, claims
Continuité	atelier, transport, ERP, fournisseur critique
Personnes	compétences rares, conflits d'intérêts

À retenir : la taxonomie donne une langue commune ; le scénario donne une exposition actionnable.

Chapitre 5 — Exploiter les informations externes et internes pour identifier les risques

L’identification robuste combine signaux externes et informations internes. Une source externe ne crée pas automatiquement un risque prioritaire : elle doit être reliée à une activité, un objectif et une exposition interne.

Externe : prix des métaux, sanctions, normes, presse économique, incidents sectoriels, cyber alertes, RJC, OCDE, FATF, Kimberley Process, ECHA, GIA, CITES, World Gold Council. Interne : incidents, plaintes, retours, inventaires, audits, pertes matière, variations de marge, retards, logs, exceptions, actions en retard.

Le World Gold Council indique qu’au T2 2026 les volumes mondiaux de demande de joaillerie en or ont reculé sous l’effet de prix élevés, tandis que la valeur dépensée est restée robuste. Ce type de signal peut affecter pricing, marges, poids moyen des produits, stock et liquidité.

La qualité du signal doit être évaluée : pertinence, fiabilité, proximité, horizon, sens de l’évolution et concordance entre sources.

À retenir : la veille enrichit l’identification, mais la priorité ne peut être conclue sans contexte interne.

Chapitre 6 — Formuler les scénarios et évaluer le risque inhérent

Le risque inhérent correspond à l’exposition avant prise en compte des contrôles. Il sert à comprendre la gravité naturelle du scénario et à décider où concentrer l’analyse des contrôles.

La matrice 5 × 5 repose sur deux axes. L’impact peut combiner finance, opérations, client, personnes, conformité, réputation, ESG et stratégie. La vraisemblance peut être exprimée à partir de fréquence historique, exposition, vulnérabilité et signaux prospectifs.

Niveau	Impact / criticité	Vraisemblance
1	faible et absorbable	rare
2	limité	peu probable
3	significatif	possible
4	majeur	probable
5	critique / stratégique	très probable ou exposition persistante

Le score Impact × Vraisemblance facilite la priorisation, mais il ne suffit pas. Ajouter vitesse du risque, criticité de l’activité, tendance, dépendance à un tiers et confiance dans les données.

À retenir : la matrice n’est pas le risque ; elle est un outil de synthèse après formulation du scénario.

Chapitre 7 — Matrice Impact × Vraisemblance et priorisation

La matrice de risque est utile lorsque les axes sont définis, les scénarios sont comparables et les limites de l’outil sont connues. Elle permet de visualiser les concentrations mais ne doit pas transformer une appréciation qualitative en fausse précision.

Pour les risques sectoriels de joaillerie, les positions montrées dans ce guide sont illustratives. Elles servent à montrer comment fonctionne la méthode. Une entreprise doit recalibrer les points avec ses expositions, valeurs de stock, incidents, marchés et contrôles.

La priorisation doit intégrer au moins : score, tendance, vitesse, appétence, concentration, obligations externes, confiance de la preuve et possibilité d’action.

À retenir : deux risques à score égal peuvent appeler des décisions différentes selon la tendance et la qualité de preuve.

Chapitre 8 — Construire l’univers des contrôles internes et des documents/preuves

Après la priorité inhérente, il faut comprendre comment l’entreprise prétend réduire le risque. Un contrôle est une activité ou mécanisme visant à prévenir, détecter ou corriger une situation qui menace un objectif.

Pour chaque contrôle clé, documenter : objectif, type, propriétaire, fréquence, population, système, données utilisées, preuve, seuil, exceptions et escalade.

Risque	Contrôles clés possibles	Preuves
Faux changement IBAN	callback + double validation	journal appel, validation, workflow
Vol / substitution	traçabilité + inventaires + accès	mouvements, comptages, logs
Sourcing	due diligence + screening + clauses	dossier tiers, screening, contrat
Prix or / marge	pricing + seuil marge + revue	fichier prix, approbation, marge
Cyber	MFA + patching + sauvegarde + monitoring	logs, tickets, rapports tests

Les documents internes à analyser incluent organigrammes, délégations, politiques, procédures, contrats, certificats, inventaires, journaux, matrices d’accès, règles de pricing, rapprochements, incidents, plans de continuité et rapports d’audit.

À retenir : une procédure n’est pas une preuve d’exécution.

Chapitre 9 — Évaluer le design et l’efficacité opérationnelle des contrôles

Le design effectiveness pose la question : si le contrôle fonctionne comme prévu, est-il suffisamment précis et complet pour réduire le risque ? L’operating effectiveness pose ensuite : fonctionne-t-il réellement de manière régulière et démontrable ?

Un contrôle peut être bien conçu mais non exécuté, ou exécuté régulièrement mais mal conçu. La conclusion résiduelle doit distinguer ces deux dimensions.

Statut	Design	Exécution	Conséquence
Efficace	adapté	démontrée	réduction crédible
Partiellement efficace	lacune limitée	irrégulière ou incomplète	réduction partielle
Inefficace	inadéquat	ou non démontrée	réduction non crédible
Non évalué	inconnu	inconnu	confiance insuffisante

Pour les contrôles automatisés, analyser aussi configuration, droits de modification, interfaces, exceptions, changements et contrôles IT généraux.

À retenir : le risque résiduel dépend de la qualité de la preuve, pas de l’existence d’un contrôle sur une procédure.

Chapitre 10 — Déterminer et visualiser le risque résiduel

Le risque résiduel est l’exposition qui subsiste après prise en compte des contrôles dont le design et le fonctionnement ont été évalués. Il ne doit pas être calculé par une simple soustraction du score inhérent.

La démarche consiste à reprendre le scénario, examiner les contrôles clés, mesurer leurs faiblesses et exceptions puis réévaluer impact et vraisemblance. L’impact peut rester très élevé même lorsque la vraisemblance diminue fortement.

Exemple : une pierre très précieuse reste un actif à impact critique. Les contrôles de coffre, traçabilité, double comptage et inventaire peuvent réduire la probabilité de perte mais pas la valeur économique de l’événement.

À retenir : l’écart entre matrice inhérente et matrice résiduelle doit être explicable par des contrôles prouvés.

Chapitre 11 — Traiter et mitiger les risques

Un risque résiduel au-dessus de l’appétence ou de la tolérance exige une réponse. ISO 31000 parle de traitement du risque. Le traitement peut éviter le risque, réduire la vraisemblance ou l’impact, transférer ou partager une partie de l’exposition, ou accepter explicitement le risque.

Une action de mitigation doit être formulée comme un changement observable : nouveau contrôle, renforcement d’un contrôle, réduction d’exposition, diversification d’un tiers, changement contractuel, automatisation, assurance ou décision de sortie.

Chaque action doit contenir propriétaire, échéance, coût, dépendances, état, preuve de clôture et effet attendu sur le risque résiduel.

À retenir : un plan d’action sans risque cible et sans preuve de clôture n’est qu’une liste de tâches.

Chapitre 12 — KRI, tendances, signaux émergents et mise à jour continue

Les Key Risk Indicators (KRI) servent à détecter une évolution de l’exposition. Un bon KRI est relié à un risque, possède une source, une fréquence, un propriétaire et des seuils de réaction.

Exemples : variation de marge brute, concentration fournisseur, nombre d’accès sensibles non revus, écart inventaire, incidents e-commerce, anomalies de retours, taux d’actions en retard, nombre de fournisseurs à forte exposition géographique.

La tendance ne doit pas être une flèche décorative. Elle doit être justifiée par une série, un signal, un changement de contrôle ou une évolution du contexte.

À retenir : le KRI mesure une exposition ou un signal ; le KPI mesure une performance. Certains indicateurs peuvent jouer les deux rôles, mais l’usage doit être explicite.

Chapitre 13 — Reporting management, direction et conseil

Le reporting n’est pas un inventaire de risques. Il doit répondre à une question de décision pour un public précis.

Audience	Ce qu'elle doit voir
Conseil / comité	top risques résiduels, tendance, appétence, décisions requises
Direction	arbitrages, actions, ressources, dépassements de tolérance
Management	risques par activité, KRI, contrôles, exceptions, échéances
Risk / contrôle interne	qualité méthode, cohérence scoring, control gaps
Audit interne	zones d'assurance, faiblesses et dépendances critiques

Un bon tableau de bord montre score actuel et précédent, tendance, confiance, contrôles faibles, actions en retard et signaux externes significatifs.

À retenir : le reporting doit conduire à une décision, une responsabilité ou une demande de preuve.

Chapitre 14 — Cas fil rouge joaillerie : de l’activité au risque résiduel

Cas : volatilité de l’or. Activités : sourcing, pricing, stock, vente et trésorerie. Signal : prix élevés et baisse des volumes de joaillerie. Scénario : la société maintient des collections trop lourdes ou des prix insuffisamment ajustés, ce qui dégrade marge et rotation du stock.

Risque inhérent illustratif : impact 4, vraisemblance 5. Contrôles : politique de pricing, fréquence de revue, seuil de marge, analyse rotation, couverture ou mécanismes d’achat selon modèle économique. Preuves : décisions pricing, fichiers prix, rapports marge, exceptions et inventaire.

Après contrôles efficaces, la vraisemblance peut être réévaluée, par exemple à 4. Le risque résiduel reste alors significatif et peut nécessiter une mitigation : collections plus légères, réduction d’exposition, fréquence de révision accrue ou seuil de marge renforcé.

Le même raisonnement s’applique au sourcing responsable, au vol, au cyber, aux matériaux de laboratoire et à la continuité fournisseur.

À retenir : le cas fil rouge montre pourquoi le traitement ne s’arrête pas au score : il suit la preuve jusqu’à une décision de management.

Chapitre 15 — Gouvernance, Trois Lignes et cadence de revue

La gouvernance définit qui possède le risque, qui challenge, qui contrôle et qui donne une assurance indépendante. Le modèle des Trois Lignes de l’Institute of Internal Auditors aide à clarifier les rôles sans supprimer les responsabilités du management.

Rôle	Responsabilité
Conseil / comité	surveillance des risques majeurs et de l'appétence
Direction	arbitrage, ressources, acceptation explicite
Managers	propriété des risques et contrôles de leurs activités
Risk / conformité / contrôle interne	méthode, challenge, consolidation, monitoring
Audit interne	assurance indépendante selon mandat

Cadence type : quotidienne pour sanctions/cyber/incidents critiques, hebdomadaire pour certains marchés et fraudes, mensuelle pour top risques et KRI, trimestrielle pour résiduel et fournisseurs, annuelle pour univers et appétence. Des événements majeurs déclenchent une revue hors cycle.

À retenir : une cartographie vivante exige une gouvernance de mise à jour aussi claire que la méthode d’évaluation.

Fiche méthode A — Définir les critères et l’appétence

Objectif : Créer des règles de décision avant de scorer les risques.

Entrées : Objectifs stratégiques, historiques de pertes, obligations, capital disponible, attentes du conseil.

Étapes : 1) définir les dimensions d’impact ; 2) définir cinq niveaux mesurables ; 3) définir la vraisemblance ; 4) préciser les zones non négociables ; 5) traduire l’appétence en tolérances et KRI.

Sortie : Risk Criteria Pack + matrice de scoring + seuils d’escalade.

Erreur fréquente : Changer les seuils après avoir vu le résultat de la heat map.

Fiche méthode B — Construire l’univers des activités

Objectif : Obtenir un référentiel stable auquel rattacher risques, contrôles, données et propriétaires.

Entrées : Organigramme, processus, systèmes, contrats, sites, canaux, catalogue de produits, chaîne d’approvisionnement.

Étapes : 1) dessiner la chaîne de valeur ; 2) ajouter les fonctions support ; 3) descendre au niveau 2/3 ; 4) identifier actifs, tiers et systèmes ; 5) nommer un propriétaire ; 6) valider la couverture.

Sortie : Activity Universe versionné.

Erreur fréquente : Confondre organigramme et univers des activités : une fonction peut participer à plusieurs processus.

Fiche méthode C — Construire l’univers des risques

Objectif : Passer d’une taxonomie générique à des scénarios reliés aux activités.

Entrées : Activity Universe, incidents, audits, sources sectorielles, objectifs, obligations.

Étapes : 1) définir les familles ; 2) rattacher chaque famille aux activités exposées ; 3) formuler cause → événement → impact ; 4) éviter doublons ; 5) attribuer un propriétaire ; 6) enregistrer les sources.

Sortie : Risk Universe + Risk Register initial.

Erreur fréquente : Écrire « cyber », « fraude » ou « ESG » comme risque sans scénario ni impact.

Fiche méthode D — Transformer un signal externe en risque

Objectif : Éviter de traiter chaque article ou alerte comme un nouveau risque.

Entrées : Source externe, Activity Universe, exposition interne, indicateurs, documents internes.

Étapes : 1) qualifier fiabilité et proximité ; 2) identifier l’activité touchée ; 3) formuler le scénario ; 4) rechercher des preuves internes ; 5) décider : créer, mettre à jour ou ignorer ; 6) tracer la décision.

Sortie : Signal-to-Risk Log avec source, justification et action.

Erreur fréquente : Confondre événement externe et exposition propre à l’entreprise.

Fiche méthode E — Scorer et prioriser le risque inhérent

Objectif : Comparer des scénarios sur des critères cohérents sans créer une fausse précision.

Entrées : Scénario, échelles impact/vraisemblance, données historiques, exposition, tendance.

Étapes : 1) scorer impact ; 2) scorer vraisemblance ; 3) calculer la position ; 4) documenter la justification ; 5) ajouter vitesse, tendance et confiance ; 6) comparer à l'appétence.

Sortie : Inherent Risk Register + heat map + liste priorisée.

Erreur fréquente : Utiliser uniquement le produit I×V pour décider.

Fiche méthode F — Construire la bibliothèque de contrôles

Objectif : Relier chaque risque prioritaire aux mesures de maîtrise qui le réduisent réellement.

Entrées : Risk Register, procédures, systèmes, documents, entretiens, contrôles existants.

Étapes : 1) identifier contrôles clés ; 2) préciser objectif et type ; 3) nommer propriétaire ; 4) définir fréquence et population ; 5) définir preuve ; 6) identifier exceptions et escalade.

Sortie : Control Library + Document/Evidence Register.

Erreur fréquente : Lister des politiques ou certifications comme contrôles sans vérifier leur exécution.

Fiche méthode G — Tester design et efficacité opérationnelle

Objectif : Distinguer le contrôle bien conçu du contrôle réellement exécuté.

Entrées : Control Library, population, preuves, logs, échantillons, exceptions.

Étapes : 1) test de design ; 2) définir population/période ; 3) sélectionner méthode de test ; 4) tester exécution ; 5) analyser exceptions ; 6) conclure et documenter confiance.

Sortie : Control Assessment avec conclusion Efficace / Partiel / Inefficace / Non évalué.

Erreur fréquente : Conclure à l’efficacité sur la base d’un entretien non corroboré.

Fiche méthode H — Évaluer le risque résiduel

Objectif : Recalculer l’exposition après contrôles prouvés et la comparer à l’appétence.

Entrées : Risque inhérent, contrôles clés, résultats de tests, exceptions, contexte actuel.

Étapes : 1) reprendre scénario ; 2) analyser réduction réelle ; 3) réévaluer impact ; 4) réévaluer vraisemblance ; 5) noter confiance ; 6) comparer à appétence/tolérance.

Sortie : Residual Risk Register + residual heat map.

Erreur fréquente : Soustraire mécaniquement un « score de contrôle » au score inhérent.

Fiche méthode I — Définir le traitement et la mitigation

Objectif : Ramener l’exposition vers un niveau accepté ou formaliser l’acceptation.

Entrées : Residual Risk Register, appétence, coûts, contraintes, options opérationnelles.

Étapes : 1) choisir éviter/réduire/transférer/accepter ; 2) définir l’action ; 3) nommer owner ; 4) fixer date ; 5) définir preuve de clôture ; 6) estimer cible ; 7) re-tester après mise en œuvre.

Sortie : Mitigation Roadmap et Target Residual Risk.

Erreur fréquente : Fermer une action quand la tâche est terminée sans vérifier l’effet sur le risque.

Fiche méthode J — Construire les KRI et le reporting

Objectif : Détecter les dérives et fournir une information décisionnelle adaptée à chaque niveau.

Entrées : Top risks, seuils, données systèmes, incidents, actions, signaux externes.

Étapes : 1) choisir un indicateur relié au risque ; 2) fixer source/fréquence/owner ; 3) définir seuils ; 4) calculer tendance ; 5) documenter confiance ; 6) adapter le reporting à l'audience.

Sortie : KRI Register + dashboard management + pack conseil.

Erreur fréquente : Multiplier les indicateurs sans seuil ni décision associée.

Conclusion — De la cartographie à l’assurance décisionnelle

La gestion des risques utile relie la compréhension de l’entreprise à une décision. Elle commence par les objectifs et les activités, utilise des informations externes et internes pour identifier les scénarios, estime le risque inhérent, évalue les contrôles et preuves, conclut sur le résiduel puis traite les expositions au-dessus de l’appétence.

Le système devient dynamique grâce aux KRI, tendances, incidents et revues. La valeur n’est pas dans le nombre de risques inscrits dans un registre mais dans la capacité à expliquer pourquoi un risque existe, comment il évolue, ce qui le réduit, ce qui reste exposé et qui doit décider.

Plan d’action — Construire le dispositif en 30 jours

Période	Action	Livrable
J1-3	objectifs, contexte, critères, appétence	Risk Criteria Pack
J4-7	univers des activités	Activity Universe
J8-10	univers des risques	Risk Universe
J11-14	sources + scénarios + scoring inhérent	Inherent Risk Register
J15-18	contrôles + documents + preuves	Control & Evidence Library
J19-22	tests design / operating effectiveness	Control Assessment
J23-25	risque résiduel + appétence	Residual Risk View
J26-27	traitement / mitigation	Mitigation Roadmap
J28-29	KRI + tendances	KRI Dashboard
J30	reporting + gouvernance	Management / Board Pack

Glossaire

Terme	Définition
Risque inhérent	exposition avant prise en compte des contrôles
Risque résiduel	exposition subsistant après contrôles évalués
Appétence	niveau global de risque que l'organisation est disposée à accepter
Tolérance	limite opérationnelle liée à un risque ou indicateur
KRI	indicateur clé de risque
Design effectiveness	capacité du contrôle à réduire le risque s'il fonctionne
Operating effectiveness	preuve que le contrôle fonctionne réellement
Traitement / mitigation	actions visant à modifier le risque ou l'exposition
Univers des activités	référentiel structuré des activités et processus
Univers des risques	taxonomie et scénarios de risques liés aux activités

Sources et références

Cadres méthodologiques : ISO 31000:2018 ; COSO Enterprise Risk Management — Integrating with Strategy and Performance (2017) ; COSO Internal Control — Integrated Framework ; IEC 31010:2019 ; IIA Three Lines.

Sources sectorielles : Responsible Jewellery Council ; OECD Due Diligence Guidance for Responsible Supply Chains of Minerals ; FATF guidance for dealers in precious metals and stones ; Kimberley Process ; ECHA ; GIA ; CITES ; World Gold Council Gold Demand Trends Q2 2026.

Note : l’applicabilité juridique doit être adaptée aux pays, produits, matières et canaux de l’entreprise. Ce livre n’est pas un avis juridique.