Procédure RCA Root Cause Analysis ISO 27001 : Template Word

15 mai 2026 • Mis à jour le 17 mai 2026 • 32 min de lecture • 3175 mots • 17 vues •

> Après un incident, l'analyse des causes racines (RCA) évite la récurrence. Ce template Word combine 5 Whys et diagramme d'Ishikawa (causes-effet) avec t.

À RETENIR

Template gratuit · Word — Procédures

Après un incident, l'analyse des causes racines (RCA) évite la récurrence. Ce template Word combine 5 Whys et diagramme d'Ishikawa (causes-effet) avec template prêt à compléter pour produire un livrable RCA conforme exigence ISO 27001 clause 10.1.

Télécharger (Word gratuit)

La **procédure d'analyse des causes racines (Root Cause Analysis — RCA)** est le mécanisme central de l'amélioration continue dans un Système de Management de la Sécurité de l'Information conforme à ISO/IEC 27001:2022. Exigée par la clause **10.1 — Amélioration continue** et la clause **10.2 — Non-conformités et actions correctives**, elle garantit que chaque incident de sécurité, non-conformité ou défaillance du SMSI donne lieu à une analyse rigoureuse des causes profondes, et non pas seulement à un traitement symptomatique. La différence est fondamentale : traiter seulement le symptôme (réinstaller un système infecté, bloquer une adresse IP malveillante) sans analyser la cause racine (pourquoi l'antivirus n'a pas détecté le malware, pourquoi l'utilisateur a cliqué sur le lien de phishing) conduit inévitablement à la récurrence de l'incident. C'est précisément ce que le clause 10.2 cherche à éviter en imposant que les non-conformités soient analysées pour déterminer leurs causes, que des actions correctives soient décidées et mises en œuvre, et que l'efficacité de ces actions soit vérifiée. Ce template Word, développé par **Ayi NEDJIMI**, consultant cybersécurité Lead Implementer ISO 27001, intègre les deux méthodologies de RCA les plus utilisées en cybersécurité : la méthode des **5 Pourquoi** (5 Whys) pour les causes simples et bien délimitées, et le **diagramme d'Ishikawa** (diagramme causes-effet ou fishbone diagram) pour les incidents complexes impliquant plusieurs catégories de causes. Il inclut également un template de rapport RCA structuré prêt à remplir, une matrice de criticité pour prioriser les RCA à réaliser, et un processus de validation des actions correctives. Il s'adresse aux RSSI et responsables sécurité qui animent les analyses post-incidents, aux chefs de projet qui gèrent les non-conformités d'audit, aux équipes IT et SOC qui contribuent à l'analyse technique, et aux auditeurs internes qui vérifient l'efficacité du processus d'amélioration