

FORMATION 06

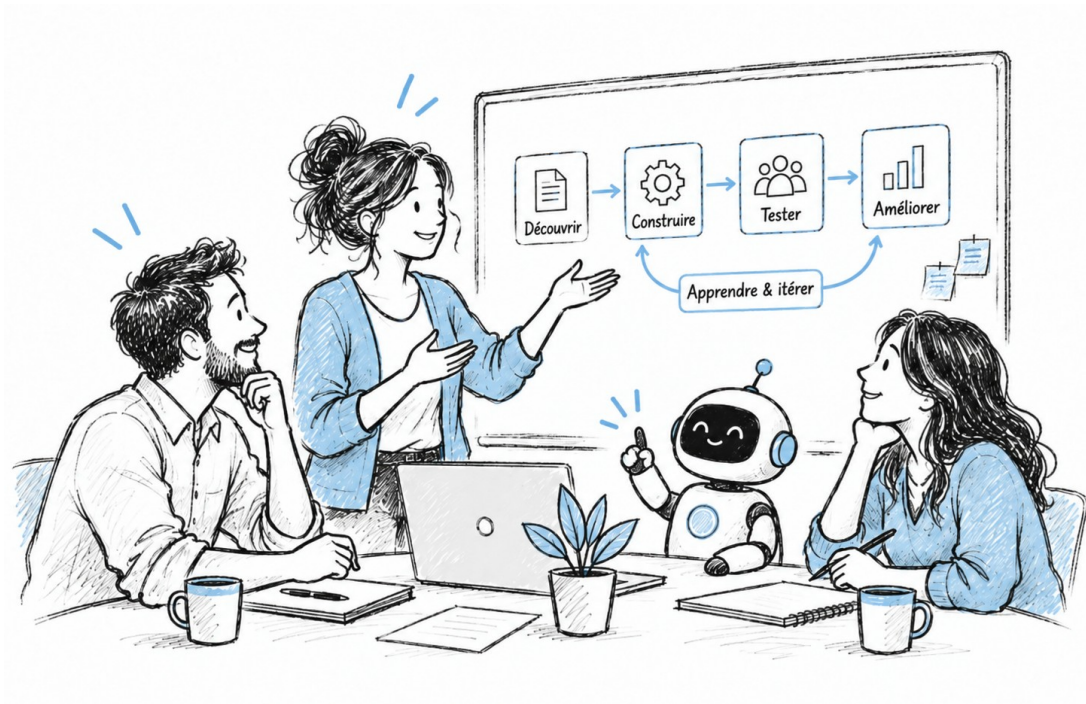
Devenir autonome sans devenir dépendant

Une automatisation utile aujourd'hui devra encore pouvoir être comprise demain.

Apprendre à documenter, superviser, exploiter et faire évoluer une automatisation afin que son fonctionnement ne repose ni sur une personne unique, ni sur un prestataire irremplaçable, ni sur une boîte noire technique.

DURÉE 7 h	GROUPE 5 à 10 participants	PRÉREQUIS Automatisation existante ou en cours de déploiement
---------------------	--------------------------------------	---

Comprendre, surveiller, reprendre, faire évoluer et transmettre ce qui a été construit.



Finalité, public et objectifs

Finalité de la formation

Cette formation aide l'entreprise à exploiter et faire évoluer ses automatisations sans concentrer toute la connaissance chez une seule personne ou un seul prestataire. Elle distingue l'usage, l'exploitation, la maintenance, la transmission et la gouvernance d'un système.

L'objectif n'est pas de rendre chaque participant capable de tout maintenir seul. Il est de rendre les dépendances visibles, choisies, documentées et réversibles, afin que l'entreprise conserve ses comptes, ses données, ses décisions et sa capacité de changement.

Résultat attendu

À l'issue de la journée, le groupe dispose d'un premier dossier d'exploitation : niveau d'autonomie, dépendances, propriétaires, documentation minimale, supervision, procédure d'incident, méthode de changement, plan de transmission et feuille de route priorisée.

Public, prérequis et modalités

Rubrique	Contenu
Public concerné	Responsables opérationnels, référents automatisation, responsables métier ou produit, équipes techniques, administrateurs, chefs de projet et dirigeants.
Prérequis	Connaissance d'une automatisation, d'un workflow, d'un agent ou d'un outil interne existant ou prochainement déployé. Aucun prérequis en développement.
Taille du groupe	5 à 10 participants recommandés ; jusqu'à 12 personnes pour un système suffisamment préparé.
Modalités	1 journée de 7 heures. Intra-entreprise recommandé. Présentiel ou visioconférence selon le contexte.
Préparation	Questionnaire en amont, documentation existante, liste des outils et comptes, exemple de journal ou d'incident, responsabilités connues.
Répartition pédagogique	Environ 35 % d'apports et 65 % d'analyse, de cartographie, d'exercices et de production documentaire.

Objectifs pédagogiques

- Distinguer utilisation, exploitation, maintenance, transmission et gouvernance.
- Évaluer le niveau d'autonomie réel de l'entreprise.
- Identifier les dépendances humaines, techniques, contractuelles et informationnelles.
- Clarifier les propriétaires, responsables, comptes, accès et données.
- Produire une documentation minimale et une supervision exploitable.
- Organiser la reprise manuelle, les changements, les versions et le retour arrière.
- Préparer la transmission à une autre personne ou à un autre prestataire.
- Définir ce que l'entreprise peut gérer seule et ce qui nécessite une compétence spécialisée.

Déroulé de la journée

La journée alterne apports méthodologiques, analyse d'un système réel ou d'un cas commun, production documentaire et exercice de reprise.

Matin - Comprendre, cartographier et documenter

Horaire	Séquence	Objectif
09:00-09:25	Autonomie, dépendance et niveau de maîtrise	Situer le système sur cinq niveaux : comprendre, surveiller, reprendre, faire évoluer, transmettre.
09:25-10:10	Cartographier les dépendances	Identifier personnes, outils, données, accès, contrats et connaissances critiques.
10:10-10:55	Propriété, comptes, accès et données	Clarifier la maîtrise des comptes, des secrets, des données et des possibilités d'export.
10:55-11:10	Pause	-
11:10-11:55	Documentation minimale utile	Construire une fiche système, un schéma, un guide d'exploitation et une procédure de reprise.
11:55-12:30	Étude d'un cas commun	Analyser une automatisation critique construite par un prestataire externe.

Après-midi - Superviser, reprendre et transmettre

Horaire	Séquence	Objectif
13:30-14:15	Superviser et détecter les anomalies	Définir indicateurs, journaux, alertes et responsables.
14:15-15:00	Incidents, reprise manuelle et continuité	Organiser l'arrêt, le mode dégradé, la correction et la reprise.
15:00-15:15	Pause	-
15:15-16:00	Faire évoluer sans casser	Prévoir sauvegarde, test, version, déploiement contrôlé et retour arrière.
16:00-16:35	Gouvernance et transmission	Répartir les responsabilités et préparer une reprise par une autre personne ou un autre prestataire.
16:35-16:55	Exercice de reprise	Gérer l'indisponibilité du créateur et plusieurs incidents simultanés.
16:55-17:00	Conclusion	Prioriser les actions à 30, 60 et 90 jours.

Contenu pédagogique - première partie

1. Échelle d'autonomie RIKŌ

Niveau	Capacité attendue	Question de contrôle
1. Comprendre	Finalité, fonctionnement, données, outils et utilisateurs sont identifiés.	Savons-nous expliquer ce que fait le système et pourquoi il existe ?
2. Surveiller	Journaux, indicateurs et alertes permettent d'identifier une anomalie.	Savons-nous vérifier qu'il fonctionne correctement ?
3. Reprendre	Arrêt, correction, reprise manuelle et escalade sont prévus.	Savons-nous continuer lorsque l'automatisation échoue ?
4. Faire évoluer	Une modification peut être testée, versionnée, déployée et annulée.	Savons-nous changer une règle sans perdre la version actuelle ?
5. Transmettre	Comptes, données, documentation et savoir-faire peuvent être repris.	Une autre personne pourrait-elle maintenir ou remplacer le système ?

2. Cartographier les dépendances

Famille	Exemples	Point de vigilance
Humaines	Créateur, référent métier, administrateur, prestataire, remplaçant.	Connaissance concentrée chez une seule personne.
Techniques	Logiciel, API, hébergement, base de données, modèle IA, messagerie.	Service difficile à remplacer ou non documenté.
Données	Fichiers, formats, historique, sauvegardes, données de référence.	Export incomplet ou données impossibles à restaurer.
Accès	Comptes, clés API, certificats, double authentification.	Compte personnel, secret non renouvelable ou accès non révocable.
Contractuelles	Abonnement, licence, durée d'engagement, limitations, conditions de sortie.	Coût, délai ou impossibilité de migration.
Connaissance	Règles métier, exceptions, procédures, historique des choix.	Savoir tacite absent de la documentation.

3. Propriété, comptes, accès et données

- Vérifier que le compte principal et les adresses administratrices appartiennent à l'entreprise.
- Distinguer propriétaires, administrateurs, utilisateurs et comptes de service.
- Centraliser les secrets dans un emplacement sécurisé, renouvelable et révocable.
- Documenter où se trouvent les données, comment les exporter et ce qui serait perdu lors d'une migration.
- Maintenir un registre des accès sans y inscrire les mots de passe.

Contenu pédagogique - deuxième partie

4. Construire une documentation minimale utile

Document	Contenu attendu
Fiche d'identité	Finalité, processus, propriétaire métier, responsable technique, criticité et utilisateurs.
Schéma de fonctionnement	Déclencheur, étapes, outils, données, décisions, sorties et points humains.
Inventaire des dépendances	Logiciels, API, comptes, contrats, personnes, données et connaissances.
Guide d'exploitation	Contrôles, journaux, erreurs courantes, suspension, relance et reprise manuelle.
Historique des changements	Date, modification, raison, auteur, version et résultats des tests.
Contacts et escalades	Responsables, remplaçants, prestataires, fournisseurs et interlocuteurs sécurité.

Principe documentaire

Une documentation utile n'a pas besoin d'être longue. Elle doit permettre à une personne qui ne connaît pas le système de comprendre sa finalité, vérifier son état, traiter les incidents courants et savoir quand demander de l'aide.

5. Cas commun - automatisation de qualification des demandes

Un système reçoit des formulaires, vérifie les informations, utilise une IA pour comprendre le sujet, attribue une priorité, crée une fiche dans un CRM, affecte la demande et notifie l'équipe.

Situation observée	Action attendue
Le compte principal appartient au prestataire.	Transférer ou partager la propriété avec l'entreprise.
La clé IA est liée à une adresse personnelle.	Créer un compte de service et une procédure de renouvellement.
Aucun export de configuration n'existe.	Mettre en place un export et vérifier sa restauration.
Les alertes arrivent à une seule personne.	Désigner un responsable et un remplaçant.
Les règles de priorité ne sont pas documentées.	Formaliser les règles et leur propriétaire métier.
Aucune reprise manuelle n'est prévue.	Définir un mode dégradé et un runbook d'incident.

Résultat recherché : l'entreprise peut continuer à travailler avec le prestataire tout en sachant surveiller le système, reprendre manuellement, révoquer les accès, récupérer les données et organiser une transmission.

Supervision, incidents et continuité

1. Superviser le fonctionnement technique et métier

Dimension	Indicateurs possibles	Responsable
Technique	Déclenchement, fin d'exécution, erreur, délai, API indisponible, quota ou authentification.	Référent technique / exploitant
Métier	Dossiers traités, dossiers bloqués, données manquantes, reprises humaines, absence anormale d'activité.	Propriétaire métier
Accès	Clé proche de l'expiration, compte désactivé, changement d'administrateur.	Administrateur
Qualité	Hausse des erreurs, résultats incohérents, dérive des règles ou des sorties IA.	Équipe métier et technique

2. Construire des alertes utiles

Événement	Seuil / fréquence	Action attendue
Erreur critique	Dès la première occurrence	Diagnostic et, si nécessaire, suspension.
Dossier bloqué	Au-delà du délai métier défini	Reprise par le responsable.
Aucune exécution	Période active sans activité	Vérification du déclencheur et des accès.
Clé proche de l'expiration	15 jours avant échéance	Renouvellement planifié.
Hausse des reprises manuelles	Revue hebdomadaire	Analyse des règles et données.

3. Procédure d'incident et mode dégradé

Étape	Action
1	Identifier l'incident et mesurer son impact.
2	Suspendre le système si la poursuite peut aggraver la situation.
3	Informar les personnes concernées et activer le fonctionnement dégradé.
4	Corriger dans un environnement maîtrisé, puis tester.
5	Reprendre le service et vérifier les dossiers en attente.
6	Documenter l'incident, ses causes et les actions préventives.

Runbook attendu

Une fiche courte doit indiquer quoi vérifier, où trouver les journaux, comment suspendre le système, quelle solution manuelle utiliser et qui contacter. Elle doit être utilisable sans solliciter immédiatement le créateur du workflow.

Faire évoluer, gouverner et transmettre

1. Modifier sans dégrader la version opérationnelle

Étape	Contrôle attendu
Besoin de changement	Objectif, impact et responsable clairement définis.
Sauvegarde / version	Version actuelle exportée et restauration vérifiée.
Modification	Travail réalisé dans un environnement sûr ou sur une copie.
Tests	Scénario nominal, erreurs et reprise contrôlés.
Validation	Propriétaire métier et responsable technique donnent leur accord.
Déploiement	Changement tracé, surveillé et réversible.
Retour arrière	Procédure, délai et autorité de décision connus.

2. Répartir les responsabilités

Activité	Métier	Exploitation	Technique	Prestataire
Définir les règles	Responsable	Consulté	Informé	Consulté
Surveiller	Informé	Responsable	Support	Support
Modifier	Valide	Consulté	Réalise	Selon contrat
Gérer un incident	Informé	Coordonne	Corrige	Support
Exporter les données	Valide	Réalise	Support	Facilite
Organiser la transmission	Responsable	Participe	Participe	Documente

3. Exercice final - le créateur n'est plus disponible

Le groupe doit gérer plusieurs événements simultanés : dossiers bloqués, clé API proche de l'expiration, règle métier à modifier et évolution annoncée par un fournisseur.

- Vérifier l'état du système et identifier les dossiers concernés.
- Retrouver la documentation, les comptes, les responsables et les contacts utiles.
- Activer un mode dégradé et maintenir la continuité du processus.
- Renouveler ou faire renouveler l'accès, puis tester la modification.
- Décider quand solliciter une compétence externe et comment transmettre le contexte.

Critère de réussite

Le groupe n'a pas besoin de résoudre techniquement chaque incident. Il doit savoir qui décide, où chercher, quoi vérifier, comment limiter l'impact, quand escalader et comment préserver la continuité.

Méthodes pédagogiques et validation des acquis

Méthodes pédagogiques

- Apports structurés et exemples issus de situations d'entreprise.
- Auto-évaluation initiale sur les cinq niveaux d'autonomie.
- Cartographie des dépendances, des comptes et des responsabilités.
- Étude d'un cas commun puis travail sur un système de l'entreprise.
- Production de supports réutilisables pour l'exploitation et la transmission.
- Exercice de reprise en l'absence du principal référent.

Critères de validation

Compétence	Manifestation attendue
Évaluer l'autonomie	Le système est positionné sur les cinq niveaux avec des justifications.
Identifier les dépendances	Les dépendances critiques et les solutions de remplacement sont cartographiées.
Clarifier la propriété	Comptes, données, responsables et possibilités de révocation sont identifiés.
Documenter	Une fiche système et un guide d'exploitation sont produits.
Superviser	Indicateurs, journaux, alertes et responsables sont définis.
Gérer un incident	Une procédure de suspension, mode dégradé et reprise existe.
Faire évoluer	Une méthode de test, version et retour arrière est proposée.
Transmettre	Un plan de reprise par une autre personne ou un autre prestataire est défini.
Prioriser	Les actions sont classées selon leur criticité et un horizon 30/60/90 jours.

Modalités d'évaluation

- Auto-évaluation initiale et finale.
- Analyse de la carte des dépendances et de la fiche système.
- Observation pendant les ateliers et l'exercice de reprise.
- Restitution orale et questionnaire de synthèse.
- Appréciation des éléments maîtrisés, à consolider ou nécessitant un spécialiste.

Livrables remis

Livrable	Contenu
Grille d'autonomie	Évaluation selon les cinq niveaux.
Fiche d'identité	Finalité, criticité, propriétaires, utilisateurs et environnement.
Carte des dépendances	Personnes, outils, données, accès, contrats et connaissances.
Registre des accès	Propriétaires, administrateurs, révocation et renouvellement.
Guide d'exploitation	Contrôles, journaux, alertes, suspension et reprise.
Procédure d'incident	Diagnostic, impact, mode dégradé, correction et vérification.
Check-list de changement	Sauvegarde, test, validation, déploiement et retour arrière.
Plan de transmission	Documents, accès, démonstration, exercice et validation de reprise.
Plan d'action	Actions prioritaires à 30, 60 et 90 jours.

Cadre, limites et prolongements

Ce que la formation ne couvre pas

La formation structure l'autonomie et la gouvernance. Elle ne remplace pas :

- un audit complet de cybersécurité, de conformité ou de continuité d'activité ;
- la correction technique de l'ensemble des automatisations ;
- une migration vers un nouveau fournisseur ou une négociation contractuelle ;
- une supervision 24 h/24 ou une architecture haute disponibilité ;
- la reconstruction de toute la documentation du système d'information ;
- la maintenance opérationnelle après la session.

Limite assumée

La journée produit une méthode, des supports et une feuille de route. Certains risques identifiés pourront ensuite nécessiter une intervention technique, juridique, de sécurité, de migration ou de transmission.

Prolongements possibles

Format	Contenu
Atelier de suivi - 2 h 30 à 3 h	Revue des actions engagées, test de la procédure d'incident, contrôle des accès, complément documentaire et priorisation suivante.
Variante approfondie - 2 jours	Inventaire d'un portefeuille d'automatisations, classement par criticité et dépendance, procédures communes, stratégie fournisseur et feuille de route.

Articulation avec le parcours RIKŌ

Formation	Contribution
Formation 01	Sélectionner les processus pertinents et le niveau d'automatisation.
Formation 02	Préparer les rôles, les équipes et la transition.
Formation 03	Concevoir un workflow clair, avec règles, exceptions et responsabilités.
Formation 04	Construire, tester, superviser et documenter une automatisation fiable.
Formation 05	Encadrer les permissions, la supervision et l'arrêt d'un agent.
Formation 06	Organiser l'exploitation, la maintenance, la transmission et la réversibilité.

Résultat attendu

À l'issue de la journée, les participants disposent d'un système mieux compris, de responsabilités clarifiées et d'une méthode pour surveiller, reprendre, faire évoluer et transmettre ce qui a été construit. L'entreprise ne devient pas capable de tout faire seule : elle devient capable de décider ce qu'elle maîtrise, ce qu'elle externalise et comment elle conserve sa liberté de choix.

Un système important doit rester compréhensible, exploitable et transmissible.

Échangeons sur votre contexte : riko-automatisation.fr/contact