Automatisation et efficacité : le parcours d'ITSAP vers ISO 27001

L'entreprise

L'entreprise O2, fondée en 1996, a su se développer et devenir n°1 des services à la personne en France, notamment grâce à sa DSI et son logiciel métier. La DSI d'O2, plus tard renommée **ITSAP**, est devenue en 2023 une ESN, spécialiste dans les **SI pour les services à la personne**, au sein du groupe Oui Care.

Le **secteur de la santé est très réglementé** : on pense notamment à **HDS** pour les hébergeurs et infogéreurs. ITSAP a donc mis en place les actions nécessaires pour garantir la fiabilité de son SI et la confiance de ses clients :

- **création d'un poste de RSSI** en 2021 ;
- lancement d'un **projet de certification** ISO 27001 et HDS.

Le RSSI & ses enjeux

Dimitri Bouron travaille au sein d'ITSAP depuis 10 ans, d'abord en tant que technicien support et administrateur système & réseaux, puis en tant que RSSI dès la **création du service sécurité il y a 3 ans et demi**.

Le RSSI partait donc d'une feuille blanche, et devait répondre à de nombreux enjeux. Parmi ceux-ci, **répondre aux exigences de certification ISO 27001 et HDS**, le tout avec une **équipe très réduite**, constituée d'une alternante et de lui-même.

Dimitri avait besoin d'une solution complète, qui lui permettrait de :

- gérer les **objectifs de sécurité et de conformité de ses multiples entités** ;
- mettre en place un **SMSI** avec toute la structure et les process associés (en particulier dans le cadre de la certification ISO 27001) ;
- protéger efficacement son organisation avec des **ressources limitées**.

L'**automatisation** et la **conformité** se présentaient donc comme les deux enjeux principaux du RSSI dans sa recherche.

Le choix de Tenacy

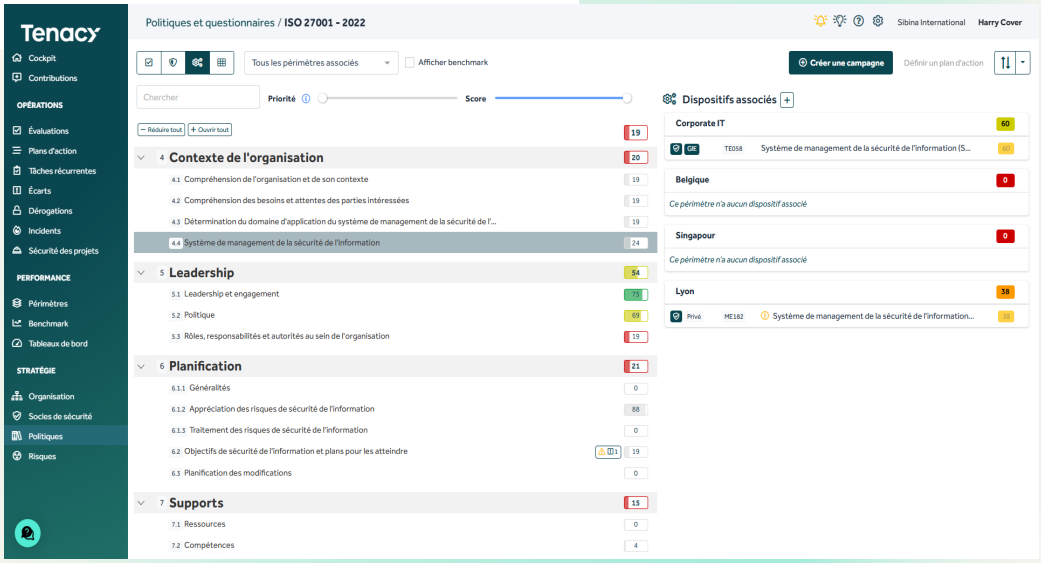
Fin 2021, ITSAP identifie qu'elle est concernée par la norme HDS sur la partie infogérance. HDS exigeant la certification ISO 27001, Dimitri Bouron (RSSI d'ITSAP) entreprend dans un premier temps de **faire auditer son SI dans la perspective de cette certification ISO 27001**.

Un **pré-audit** est mené pour identifier le niveau de maturité de l'entreprise vis-à-vis des exigences de la norme – un investissement conséquent, puisqu'une telle prestation peut coûter entre 5 000 et 10 000 euros.

Or, **quelques mois après cet audit, ISO 27001 change de version**. Il ne serait plus possible de se faire certifier sur la version 2013. Par ricochet, une nouvelle certification HDS devenait impossible pour ITSAP, celle-ci exigeant alors encore ISO 27001:2013.

Le RSSI devait repartir d'une feuille blanche, une situation compliquée qui lui a fait réaliser qu'il avait **besoin d'une solution pour rationaliser sa conformité**.

> « **Un pré-audit HDS/ISO 27001 coûte entre 5 000 et 10 000 euros**, voire jusqu'à 20 000 avec accompagnement. **Grâce à Tenacy, j'ai pu m'auto-évaluer de manière guidée** et réduire ces dépenses tout en restant efficace. »



Étape 1 : l'auto-évaluation

Dimitri ne souhaitait pas repasser de pré-audit tout de suite, sans garantie que son contexte serait bien compris, ni que les bonnes clés d'amélioration lui seraient fournies. Le RSSI a donc commencé par une **auto-évaluation via Tenacy, qui lui a permis d'évaluer son degré de maturité vis-à-vis des exigences d'ISO 27001** – mais aussi d'obtenir un **plan d'action adapté** pour guider ses efforts de mise en conformité et structurer ses process.

> « Tenacy m'a permis de construire et formaliser un SMSI complet en partant de rien en seulement un an. »

> « Un intérêt clé de Tenacy réside dans sa capacité à permettre une auto-évaluation guidée. La plateforme affiche les mesures de sécurité associées à chaque exigence, ce qui aide à comprendre où on se situe sans avoir besoin d'un avis externe à chaque étape. »

Le bonus : Tenacy inclut à la fois ISO 27001, ISO 27002 et HDS (et bien d'autres référentiels !). Chaque texte est modélisé sur un catalogue commun de mesures de sécurité. Grâce à cette approche multi-conformité, il ne vous faut qu'une minute à la mise à jour d'un texte pour voir ce à quoi vous êtes toujours conforme – et ce qu'il vous reste à faire.

Dans un premier temps, le RSSI a choisi de baser son évaluation de maturité sur l'existence (ou l'absence) chez ITSAP des mesures de sécurité exigées par ISO 27001. Cet inventaire des mesures existantes a permis à Dimitri de bénéficier dans Tenacy d'un **premier score de conformité**, et d'un **plan d'action clair** sur les mesures de sécurité à mettre en place dans le cadre de la certification.

Étape 2 : le plan d'action

Au bout d'un an et demi, ayant implémenté l'ensemble des mesures de sécurité requises, Dimitri a **mené une autre auto-évaluation**, cette fois-ci dans l'optique de challenger l'efficacité des mesures de sécurité implémentées, et d'ainsi obtenir un score de conformité plus précis et fiable.

À partir de ces résultats et des **suggestions fournies par la plateforme Tenacy**, le RSSI a élaboré un plan d'action pour améliorer l'efficacité de ses mesures de sécurité. Un exemple d'amélioration : Dimitri a conçu une nouvelle méthode de pilotage des risques basée sur Ebios RM et ISO 27005 et exploitant Tenacy. Cela lui a donné plus de flexibilité dans ses analyses et permettait de répondre d'ores et déjà aux exigences de HDS.

Zoom sur les contrôles permanents

La plateforme permet également un suivi des contrôles permanents (appelées tâches récurrentes) à effectuer dans le cadre de la mise en conformité avec un formalisme clair :

- La tâche a-t-elle été faite ?
- Le contrôle a-t-il donné le résultat attendu ?

Le **score de conformité est mis à jour en temps réel en fonction des résultats de ces contrôles**. Tenacy offre ainsi à ITSAP une **visibilité quotidienne sur les progrès de sa conformité**. Le lien entre les opérations quotidiennes et les scores aide aussi à se prémunir contre un éventuel faux sentiment de sécurité : ce n'est pas seulement l'existence des mesures qui est prise en compte, mais bien leur efficacité dans la protection de l'organisation.

Le bonus : le RSSI peut collaborer avec les équipes infrastructure et support, qui saisissent quelques réponses dans Tenacy (par exemple, indiquer si le nettoyage des comptes dormants sur Google a été effectué ou non). Dimitri peut ainsi vérifier ce qui a été fait, consulter l'historique de chaque élément, et effectuer les relances nécessaires.

Zoom sur l'automatisation

Garder un oeil vigilant sur sa conformité requiert de nombreux indicateurs, souvent éparpillés entre de multiples outils. Tenacy permet de centraliser ces métriques, et même de les automatiser, comme l'a fait Dimitri en tirant profit de l'API de Tenacy. En rédigeant différents scripts, le RSSI a automatisé la remontée de ses indicateurs. Ses tableaux de bord Tenacy sont ainsi mis à jour sans aucune intervention nécessaire de sa part.

Une fonction très utile pour les revues SMSI que Dimitri présente lors des comités de pilotage. Avant Tenacy, le RSSI devait exporter les résultats bruts dans Google Sheets, faire des traitements de calcul, tout mettre au bon format, puis insérer dans ses slides – un travail très chronophage, qui pouvait prendre jusqu'à une semaine. **À présent, il n'a plus qu'à copier/coller les graphiques générés dans Tenacy sur sa présentation. En 30 minutes, tout est prêt !**

> « Grâce à Tenacy, j'ai quasiment décuplé ma capacité à obtenir une certification. Ce qui me prenait des jours auparavant pour saisir manuellement les métriques ne prend plus que 30 minutes. »

Dimitri peut ainsi consacrer son temps à l'analyse de ces résultats (explications, actions à mettre en place...), qui constitue sa véritable valeur ajoutée en tant que RSSI. L'expert gagne du temps, un temps qu'il peut investir pour faire son « vrai » métier.

> « L'automatisation dans Tenacy m'a permis d'éliminer des tâches répétitives. Là où je faisais tout manuellement avant, aujourd'hui, je peux consacrer mon énergie à l'interprétation des résultats et à la prise de décision. »

Étape 3 : la certification

L'objectif de Dimitri ? **Demander un pré-audit ISO 27001 fin 2025**, pour une certification à l'horizon 2026. Le RSSI n'a plus besoin de faire de pré-audits réguliers : il peut suivre l'évolution de ses efforts sur Tenacy et choisir LE moment où tout lui semble prêt.

Dimitri et son adjointe s'attaquent en parallèle à la **certification HDS 2.0**, sortie récemment et exigeant cette fois-ci ISO 27001:2022. Grâce à la **modélisation des frameworks** disponible dans Tenacy et à l'angle **multi-conformité** de la plateforme, l'équipe SSI visualise simplement ce qu'il lui reste à faire une fois les exigences d'ISO 27001 satisfaites.

Avec Tenacy, une équipe de deux experts est ainsi en mesure de gérer de multiples conformités sur plusieurs périmètres.

> « Personnellement, je vois difficilement comment, en étant seul, j'aurais pu gérer toute la charge de travail liée à l'évaluation de la performance et au pilotage du SMSI. Tenacy simplifie et réalise énormément de choses qu'il aurait fallu gérer manuellement sur Excel, comme les tableaux de bord et les évaluations de performance, tout en guidant le processus. »

Grâce à Tenacy, le RSSI d'ITSAP est en mesure de gérer plusieurs conformités, de faire des reportings précis, et de gagner du temps au quotidien. La preuve qu'on peut faire beaucoup (de protection) avec peu (de ressources humaines), si on est bien équipé !

Réservez votre démo pour en savoir plus !