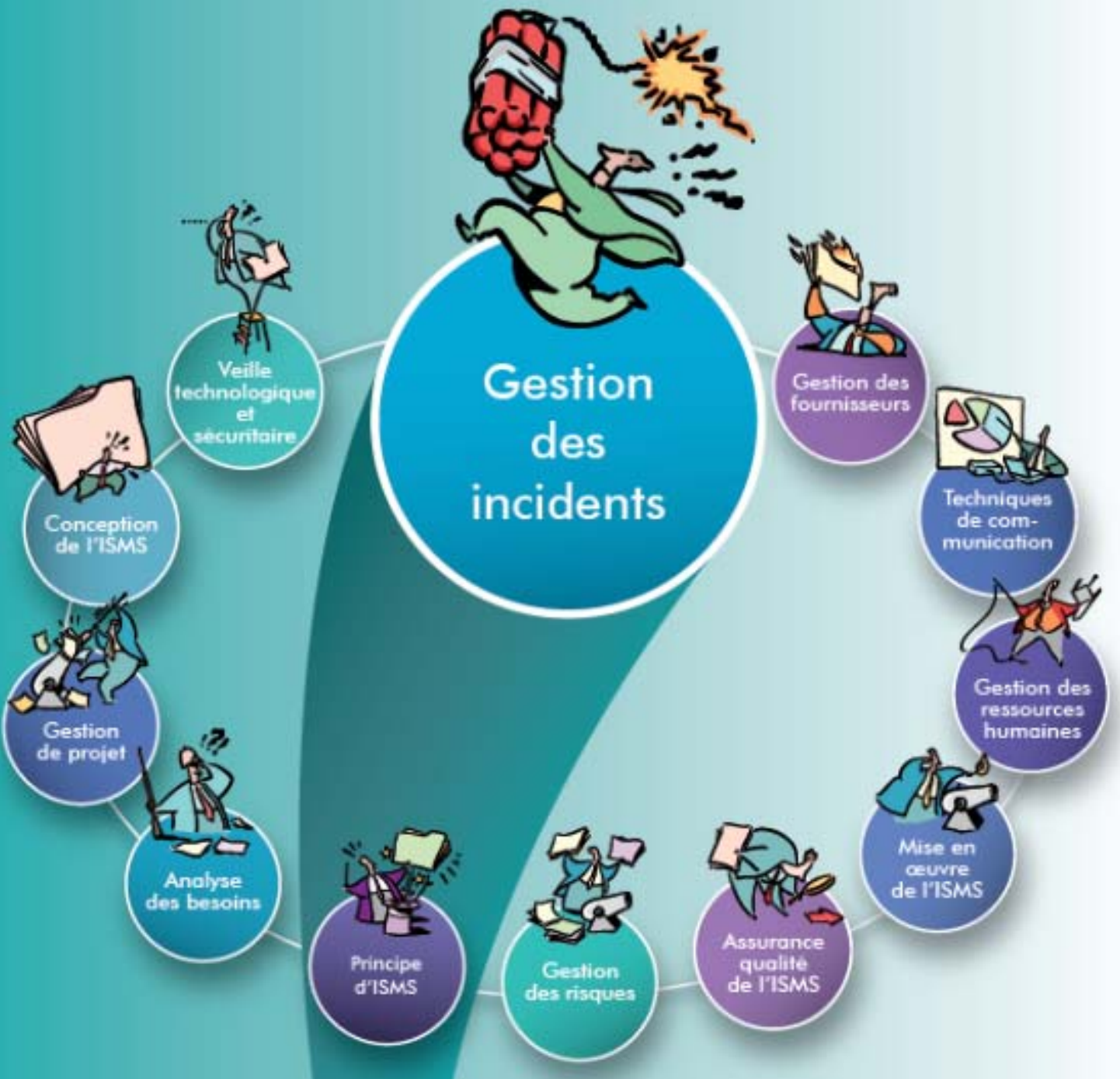
IDEC école supérieure d'informatique

ICT Security Expert

# Gestion des incidents et de la continuité d'activité



# Sommaire

**Chapitre 4**

# Introduction

Quelles que soient leur taille et leur activité – de la petite entreprise à la multinationale, de la chaîne de magasins à l'administration fédérale – toutes les organisations sont confrontées à la gestion des incidents qui impactent leur système d'information.

Ces incidents peuvent être de faible importance mais aussi bien peuvent entraîner une crise majeure voire la disparition de l'organisation si la perte financière est trop élevée.

La manière de gérer les incidents est l'un des principaux indicateurs du niveau de maturité d'une organisation dans l'exploitation de son système d'information.

Une organisation qui aura mis en place un ISMS[1] conforme ISO 27001:2013 – dont le principe est résumé ci-contre – peut s'attendre à gérer moins d'incidents qu'une autre qui ne se préoccupe guère de sécurité des systèmes d'information (SSI). Cependant, aucune contre-mesure ne pouvant prétendre protéger entièrement un actif informationnel, des incidents surviendront toujours, et d'autant plus que les menaces évoluent constamment.

Elaborer un processus capable d'identifier, de catégoriser et de traiter les incidents s'avère donc essentiel pour toute organisation qui possède un système d'information (SI), autrement dit toutes les organisations, y compris celles dont le SI est encore essentiellement sous forme papier ou intangible[2]. Gardons bien à l'esprit que la SSI s'intéresse à l'ensemble des informations, indépendamment de leur forme.

La plupart du temps, les incidents n'entraînent pas des conséquences telles que le SI de l'organisation cesse partiellement ou totalement de fonctionner. Toutefois, de tels incidents peuvent survenir à tout moment et, là encore, c'est la préparation qui fera la différence : posséder un plan de continuité d'activité, même succinct, évite que l'incident majeur provoque la panique et permet de ramener la durée de l'indisponibilité à ce qui est supportable pour l'organisation touchée et son écosystème (clients, fournisseurs, partenaires, etc.)

---

[1] Tous les mots soulignés en pointillés sont définis dans le lexique, page 15 et suivantes.

[2] Des informations souvent essentielles, voire critiques, n'existent parfois que dans la mémoire des personnes qui possèdent certaines compétences ou habilitations. Considérée comme indispensable au point que certains parcourent des centaines de kilomètres pour assister à une réunion, la communication verbale véhicule aussi des informations dont la transposition sur un support matériel n'est pas toujours assurée de manière correcte et complète (intègre).

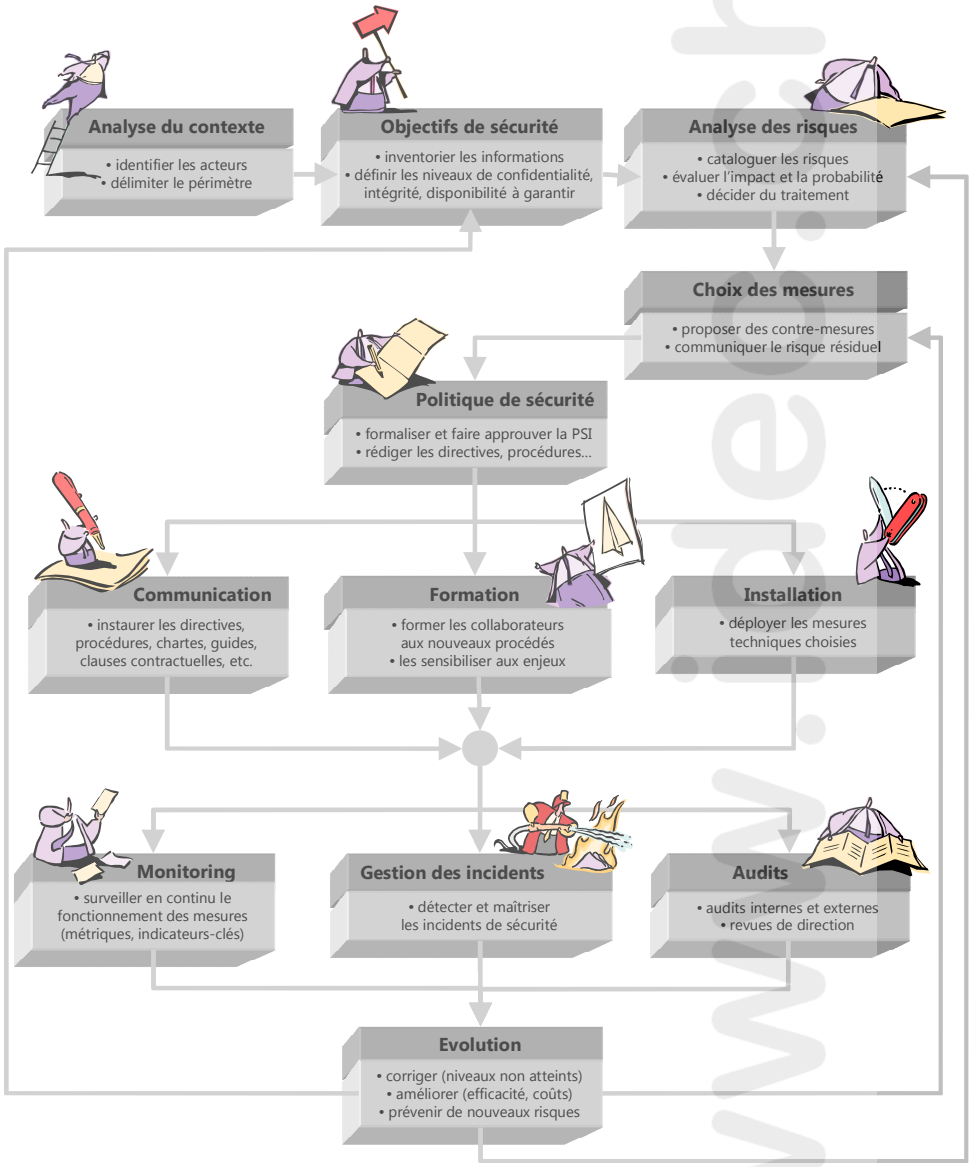



*Figure 1 : principales activités de construction et d'exploitation d'un ISMS*

Par rapport au précédent schéma, le présent ouvrage couvre spécifiquement l'étape de gestion des incidents et aborde également l'étape d'évolution, dans l'approche PDCA aujourd'hui indissociable de l'ISMS, ainsi que les étapes préliminaires à l'élaboration d'un processus de gestion des incidents : analyse du contexte, définition des besoins (objectifs de sécurité), gestion des risques, choix et mise en œuvre de mesures préventives.

Le premier chapitre forme la pierre angulaire de la gestion des incidents et de la continuité d'activité : c'est l'analyse de l'impact métier – *business impact analysis* (BIA) – qui permet d'assigner une priorité de traitement à un incident et fixe le délai maximal pour restaurer la disponibilité d'un actif informationnel.

Le second chapitre fournit des recommandations pour élaborer un processus de gestion des incidents qui soit en adéquation avec les besoins de l'organisation : la criticité du SI pour l'accomplissement de sa mission mais aussi la nature des informations traitées avec les contraintes légales et règlementaires qui en découlent, son niveau de tolérance au risque (*risk appetite*)…

Dans le troisième chapitre, des étapes de conception d'un plan de continuité d'activité (PCA) sont proposées.

Enfin, le dernier chapitre s'intéresse à l'autre pierre angulaire de la gestion des incidents et de la continuité d'activité : les ressources humaines, qui constituent un facteur clé de réussite de ces processus. Dans ce domaine, les plans et les mesures techniques – aussi parfaits soient-ils – ne servent à rien si les employés de l'organisation ne sont pas formés à réagir en cas d'incident, ne sont pas entraînés à accomplir leurs tâches respectives si le plan de continuité d'activité doit être déclenché.

Au fil des chapitres, nous voyagerons en compagnie de trois entreprises fictives mais réalistes qui doivent s'assurer de l'adéquation entre leurs besoins et leur politique SSI et dont les expériences illustreront certaines notions.

La première est une petite entreprise qui développe des logiciels de *serious games*, des jeux à vocation éducative destinés à la formation en entreprise. Son fondateur, propriétaire et directeur se nomme David Vinssant et il a créé son entreprise après plusieurs années de carrière en tant que consultant SSI. Durant ses loisirs, David a conçu plusieurs jeux gratuits qui ont obtenu un honorable succès sur les plateformes de téléchargement. L'idée lui est alors venue de conjuguer son hobby et sa profession afin de réaliser un *serious game* de sensibilisation à la SSI. Il a donc fondé David Vinssant Développement Logiciel (**DVDL**). Afin de se montrer exemplaire vis-à-vis de sa clientèle, DVDL est certifiée ISO 27001. Son produit, CyberSecurity Serious Game (CSSG) est disponible en SaaS ou *on premise*. DVDL développe également des solutions sur mesure. Le risque majeur pour DVDL serait qu'une faille dans ses logiciels permette l'intrusion dans le SI de ses clients. Pour s'en prémunir autant que possible, le développement s'effectue selon les bonnes pratiques DevSecOps. Toutes les spécifications fonctionnelles sont accompagnées de spécifications sécuritaires (niveaux d'authentification et de cryptage requis, par exemple) et le pipeline de développement est instrumenté avec des outils de fuzzing pour les tests et un scanner de signatures YARA visant les composants Open Source obtenus à partir de tiers. Pour DVDL, l'exploitation d'une faille logicielle constituerait le plus grave des incidents.

Notre seconde entreprise est bien loin de la PME puisqu'il s'agit de la banque Koffr-Faure qui emploie près de 10'000 collaborateurs dans un réseau d'agences couvrant toute la Suisse. Face à la méfiance grandissante de la clientèle vis-à-vis de la cybercriminali-

té et de l'usage des données personnelles, la banque souhaite se positionner comme un partenaire de confiance en démontrant la conformité de son ISMS à la norme de sécurité internationale ISO 27001. Cela suppose beaucoup d'investissements pour mettre à niveau l'existant et la direction ne s'attend pas à atteindre cet objectif à court terme. Cependant, tous les nouveaux projets doivent être entièrement conformes ISO 27001, particulièrement le guichet numérique qui vient d'être lancé afin de permettre à ceux qui le souhaitent de gérer toute leur relation avec la banque à partir d'un smartphone, y compris l'ouverture de comptes.

Enfin, notre troisième entreprise est un fournisseur d'électricité, éNergies Réunies Vaudoises SA (**NRV**), société née de la fusion de plusieurs producteurs et distributeurs locaux au moment de la libéralisation du marché de l'électricité. NRV vient de débuter un projet majeur : remplacer tous les compteurs d'électricité traditionnels par des compteurs intelligents et connectés nommés Smart-E. Non seulement les compteurs Smart-E pourront effectuer les relevés à distance mais ils pourront aussi être consultés directement par les clients désireux de connaître leur consommation en temps réel afin d'éviter les mauvaises surprises lors de la réception des factures. L'analyse des données de consommation doit aussi permettre de conseiller le client sur la nature de son abonnement et sur les plus énergivores de ses équipements. Echaudée récemment par une intrusion dans ses systèmes SCADA, NRV est résolue à proposer des compteurs « *secured by design* », c'est-à-dire intégrés dans une architecture de sécurité qui protège les données personnelles des clients et empêche toute utilisation dévoyée. S'il est prévu d'anonymiser les données pour les stocker de manière centralisée, chaque Smart-E héberge cependant des informations hautement personnelles : l'emplacement du compteur identifie clairement l'habitation concernée et ses données de consommation indiquent les horaires habituels des habitants ainsi que la nature des équipements qu'ils possèdent, soit des informations très utiles