EXCELLENCE.
COMPÉTENCE.
RECONNAISSANCE.

ISO 22301
SÉCURITÉ SOCIÉTALE
SYSTÈMES DE GESTION
DE LA CONTINUITÉ DES ACTIVITÉ

Livre Blanc

Sécurité sociétale
Systèmes de Gestion de la Continuité des Activité

PRINCIPAUX AUTEURS

René St-GERMAIN, PECB (France)
Faton ALIU, PECB (Canada)
Eric LACHAPELLE , PECB (Canada)
Pierre DEWEZ , Devoteam (Belgique)

LISTE DES CONTRIBUTEURS

Daniela CATALIN, IT Academy (Roumanie)
Goran CHAMUROVSKI, INTEGRA Solution (Macedonia)
Jacques CHENEVIERE, Devoteam (France)
Marcelo CORREA, Behaviour (Brésil)
Karsten M. DECKER, Decker Consulting (Suisse)
Jérôme FERRU, Devoteam (France)
Karim HAMDAOUI, LMPS Consulting (Maroc)
Mathieu LACHAINE, Kereon (Canada)
Jan MAES, Devoteam (Belgique)
Simona MOSTEANU (Belgique)
Graeme PARKER, Parker Solutions (UK)
Dirk PAUWELS, Devoteam (Belgique)
Joaquim PEREIRA, Behaviour (Portugal)
Sébastien RABAUD, SCASSI (France)
Itzhak SHARON, GSECTRA (Israel)
François TÊTE, Devoteam (France)
Gilles TROUESSIN, SCASSI (France)
Alexandrine VILLE, SEKOIA (France)
Richard G. WILSHER, Zygma (États-Unis)

TABLE DES MATIÈRES

|| INTRODUCTION

Les récentes catastrophes naturelles, les accidents environnementaux, des accidents technologiques et des crises artificielles ont montré que de nombreux incidents sont susceptibles de survenir, touchant tous les secteurs, tant public que privé. Le défi à relever va au-delà de la simple fourniture d'un plan d'intervention d'urgence ou du seul recours à des stratégies de gestion des catastrophes qui ont été employées précédemment.

Les organisations de toutes tailles et de tous types doivent maintenant s'engager dans un processus complet et systématique de prévention, protection, préparation, atténuation, et d'intervention, de continuité et de récupération. Il ne suffit plus de rédiger un plan d'intervention qui anticipe et minimise les conséquences des ruptures naturellement, accidentellement ou intentionnellement provoquées, mais il s'agit plutôt pour les organisations d'également prendre des mesures proactives d'adaptation afin de minimiser la probabilité d'une perturbation. Les menaces d'aujourd'hui nécessitent la création d'un processus continu, dynamique et interactif qui assure la survie et la durabilité des activités de base d'une organisation avant, pendant, et après un événement perturbateur.

La capacité d'une organisation à se remettre d'une catastrophe est directement liée au degré de planification de la continuité de l'activité qui se déroulait normalement avant la catastrophe. Les analystes du secteur affirment que deux entreprises sur cinq qui subissent une catastrophe risquent la faillite dans les cinq ans qui suivent l'événement.

Les plans de continuité des activités sont essentiels au fonctionnement transparent et continu de tous les types d'entreprises. Plus important encore, ces stratégies revêtent une importance accrue car les entreprises deviennent de plus en plus dépendantes de la technologie pour réaliser leurs affaires. Alors que ces entreprises mettent davantage l'accent sur l'informatique et les services de communications - afin de soutenir leurs transactions avec leurs clients ou de gérer leurs chaînes d'approvisionnement - elles deviennent de moins en moins tolérantes à la perte d'informations ou de services suite à une catastrophe.

Malgré la clarté du fait que les arrêts non maîtrisés soient catastrophiques, l'institut de recherche Gartner indique que moins de 30 pour cent des compagnies du Fortune 2000 ont investi dans un plan complet de continuité de l'activité. La raison de cette négligence peut être simplement liée aux défis techniques qui semblent trop ardus ou, peut-être, au coût de mise en œuvre perçu comme trop important. Ces préoccupations sont évidemment justifiées mais elles peuvent être assez aisément adressées par des solutions de continuité des activités.

ISO 22301, la première norme internationale de gestion de continuité des activités (GCA ou BCM, « Business Continuity Management »), a été développée pour aider les organisations à minimiser les risques liés à de telles perturbations. L'ISO a officiellement lancé la norme ISO 22301, « Sécurité sociétale - Systèmes de Gestion de la Continuité des Activités – Exigences », qui devient le nouveau standard de facto pour la gestion de la continuité des activités. Cette norme remplace donc l'actuel standard britannique BS-25999.

Selon une étude menée par le groupe META, la perte financière potentielle liée au temps d'arrêt est stupéfiante. Pour un détaillant en ligne, la perte horaire serait ainsi de plus d'un million de dollars, en moyenne.
Pour une institution financière, la perte moyenne horaire serait quant à elle plus proche du million et demi de dollars. Et pour les entreprises des services publics tels que les télécommunications et l'énergie, la perte potentielle pourrait même atteindre les 2,8 millions de dollars à l'heure, soit plus de 67 millions de dollars par jour ou, 24,5 milliards de dollars sur un an.

|| APERÇU D'ISO 22301:2012

ISO 22301 spécifie les exigences pour planifier, déployer, mettre en œuvre, exploiter, surveiller, revoir, maintenir et améliorer en permanence un système de gestion documenté pour permettre de réduire la probabilité d'occurrence d'un événement désastreux, s'y préparer, intervenir et récupérer à la suite de la survenance d'incidents perturbateurs quels qu'ils soient.

Les exigences spécifiées dans la norme ISO 22301 sont génériques et prévues pour s'appliquer à toutes les organisations (ou parties de celles-ci), indépendamment du type, de la taille et de la nature de l'organisation. La portée d'application de ces exigences dépend de l'environnement opérationnel de l'organisation et de sa complexité.

La normalisation de la continuité des activités évolue avec la norme ISO 22301 par l'ajout, notamment:

- De l'accent qui est mis sur la définition des objectifs, du suivi des performances et des indicateurs de mesure de celles-ci;
- Des attentes plus claires en matière de gestion;
- D'une planification plus soignée et d'une meilleure préparation des ressources nécessaires pour assurer la continuité des activités;

ISO 22301 s'applique à toutes les organisations qui souhaitent:

1. établir, mettre en œuvre, maintenir et améliorer un SMCA;
2. assurer la conformité avec la politique de continuité des activités;
3. démontrer la conformité à des tiers;
4. obtenir la certification / l'enregistrement de son SMCA par un organisme de certification indépendant;
5. déposer une auto-détermination et une auto-déclaration de conformité à cette norme internationale.

Qu'est-ce qu'un système de management de la continuité d'activité ?

Le SMCA est un processus de gestion globale qui identifie les menaces potentielles pour l'organisation et les impacts de ces menaces sur les opérations commerciales. Ce système de management fournit un cadre pour la construction de la résilience organisationnelle d'une organisation avec une capacité efficace de riposte qui préserve les intérêts de ses principales parties prenantes, sa réputation, sa marque et la valeur qu'elle génère.

ISO 22301 est la première norme à être entièrement compatible avec les nouvelles lignes directrices de l'ISO / Guide 83 (structure à haut niveau et texte identique pour les standards des systèmes de management et terminologie de base et définitions communes pour les systèmes de management). Ce guide a été développé en réponse aux critiques des utilisateurs de ces standards selon lesquels, tandis que les normes actuelles ont de nombreux éléments communs, celles-ci n'étant pas suffisamment alignées, il devient de plus en plus difficile pour les organisations de rationaliser leurs systèmes en les intégrant dans une seule interface.

Cela signifie que la norme ISO 22301 sera la première norme à intégrer pleinement une structure de haut niveau et un texte commun qui la rendra totalement alignée avec tous les autres systèmes de management.

Clauses essentielles de l'ISO 22301:2012

Suite à la nouvelle structure du guide ISO 83, les exigences de l'ISO 22301 sont structurées au sein des clauses suivantes:

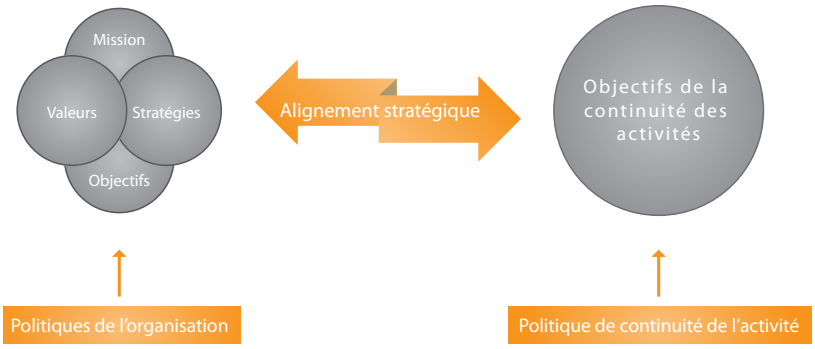
Clause 4: Contexte de l'organisme
Clause 5: Leadership
Clause 6: Planification
Clause 7: Support
Clause 8: Gestion des opérations
Clause 9: Evaluation de performance
Clause 10: Améliorations

Chacune de ces activités-clés est détaillée ci-après.

|| CLAUSE 4: CONTEXTE DE L'ORGANISATION

Déterminer les enjeux internes et externes qui sont pertinents pour atteindre l'objectif et qui affectent la capacité de l'organisation à atteindre les résultats escomptés de son SMCA:

- les activités de l'organisation, ses fonctions, ses services, ses produits, ses partenariats, les chaînes d'approvisionnement qu'elle fait fonctionner, ses relations avec les parties intéressées, et l'impact potentiel lié à un événement perturbateur;
- les liens entre la politique de continuité des activités et les objectifs de l'organisation ainsi que les autres politiques, y compris la stratégie
- globale de gestion des risques;
- l'appétence de l'organisation pour le risque;
- les parties intéressées les plus pertinentes et leurs exigences;
- contexte légal et régulatoire applicables ou tout autre contexte ou ensemble d'exigences auxquels adhère l'organisation;



|| CLAUSE 5: LEADERSHIP

La direction de l'organisation doit faire preuve d'un engagement continu envers le système de gestion de continuité de l'activité. Grâce à son leadership, la direction peut créer un environnement dans lequel les différents acteurs sont pleinement impliqués et dans lequel le système de gestion peut fonctionner efficacement, en synergie avec les objectifs de l'organisation. Le management est ainsi responsable de:

- assurer que le SMCA est compatible avec l'orientation stratégique de l'organisation;
- intégrer les exigences du SMCA dans les processus métier de l'organisation;
- définir les critères d'acceptation des risques et les niveaux de risque acceptables;
- établir et communiquer une politique de continuité des activités;
- veiller à l'affectation des responsabilités et de l'autorité des différents rôles pertinents;
- communiquer l'importance d'une gestion efficace de la continuité des activités;
- veiller à ce que le SMCA atteigne les résultats escomptés;
- orienter et soutenir l'amélioration continue;
- fournir les ressources nécessaires au SMCA;

|| CLAUSE 6: PLANIFICATION

Il s'agit d'une étape cruciale en ce qui concerne l'établissement d'objectifs stratégiques et des principes directeurs du SMCA dans son ensemble. Les objectifs d'un système de gestion de la continuité de l'activité sont l'expression de l'intention de l'organisation de traiter les risques identifiés et / ou de se conformer aux exigences des besoins organisationnels. Les objectifs de continuité de l'activité doivent:

- être cohérents avec la politique de continuité d'activité;
- tenir compte du niveau minimum acceptable de produits et de services nécessaires à l'organisation pour qu'elle puisse atteindre ses objectifs;
- être mesurables;
- tenir compte des exigences applicables;
- être surveillés et tenus à jour de façon appropriée;

|| CLAUSE 7: SUPPORT

La gestion au jour le jour d'un système de management de la continuité efficace repose sur l'utilisation des ressources appropriées pour chaque tâche. Il s'agit notamment de disposer de personnel compétent, formé et accompagné (de façon démontrable), ainsi que d'une démarche de sensibilisation et d'un plan de communication solides. Ces éléments doivent bien sûr être étayés par des informations documentées et correctement gérées.
Dans cette optique, tant les communications internes qu'externes de l'organisation doivent être considérées dans le périmètre, en ce compris leur format, leur contenu et le calendrier de celles-ci. Une planification adéquate du SMCA est donc également très importante à ce stade.

Les bonnes pratiques de documentation d'un SMCA exigent également le respect des exigences standards pour les systèmes de management, en ce compris pour la création, la modification et le contrôle des documents.

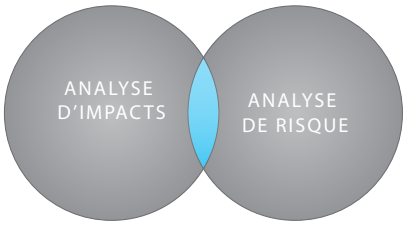
|| CLAUSE 8: GESTION DES OPÉRATIONS

Après avoir planifié le SMCA, une organisation doit le mettre en opération. Cette clause comprend les éléments suivants:

>> **Analyse d'impacts ou Business Impact Analysis (BIA):** Cette activité permet à une organisation d'identifier les processus critiques qui soutiennent la production de ses principaux produits et services, les interdépendances entre les processus et les ressources nécessaires pour faire fonctionner les processus à un niveau minimum acceptable.

>> **Analyse de risque :** ISO 22301 propose de se référer à la norme ISO 31000 pour mettre en œuvre ce processus. Le but de cette exigence est d'établir, de mettre en œuvre, et de maintenir un processus formel d'évaluation des risques documenté qui identifie de façon systématique, analyse et évalue le niveau de risque d'incidents perturbateurs vis-à-vis de l'organisation.

Processus qui consiste à identifier et mesurer l'impact sur l'activité ou les pertes dans les processus métiers en cas de perturbation



Processus systématique d'identification, d'analyse et d'évaluation du risque

>> **Stratégie de continuité de l'activité :** Une fois que les exigences ont été établies par l'analyse d'impacts et l'évaluation des risques, des stratégies peuvent être développées pour identifier les dispositions qui permettront à l'organisation de protéger et d'assurer la continuité des activités critiques fondées sur la tolérance des risques organisationnels, à l'intérieur d'objectifs définis en temps de récupération. L'expérience et les bonnes pratiques indiquent clairement que la mise en œuvre rapide d'une stratégie globale de continuité de l'activité permet de s'assurer que les activités du SMCA sont alignées avec la stratégie globale de l'organisation. La stratégie de continuité d'activité devrait être partie intégrante de la stratégie d'entreprise d'une institution.

>> **Procédures de la continuité de l'activité:** L'organisation doit documenter les procédures, y compris les dispositions nécessaires pour assurer la continuité des activités et la gestion d'un incident perturbateur. Les procédures doivent :

- o établir un protocole approprié de communications interne et externe;
- o être précises en ce qui concerne les mesures immédiates qui doivent être prises lors d'une interruption;
- o faire preuve de souplesse pour répondre aux menaces imprévues et à l'évolution des conditions internes et externes;
- o mettre l'accent sur l'impact des événements qui pourraient perturber l'exploitation;
- o être développé sur la base des hypothèses énoncées et une analyse des interdépendances;
- o être efficace en minimisant les conséquences à travers la mise en œuvre de stratégies appropriées d'atténuation d'impacts.

>> **Tests et exercices :** Pour s'assurer que les procédures de continuité d'activité sont conformes aux objectifs, une organisation devra les valider régulièrement. Les exercices et les tests sont des processus de validation des plans de continuité des activités et de leurs procédures associées pour s'assurer que les stratégies choisies sont capables de fournir des réponses et des résultats de la récupération dans les délais convenus par la Direction.

|| CLAUSE 9: ÉVALUATION DE LA PERFORMANCE

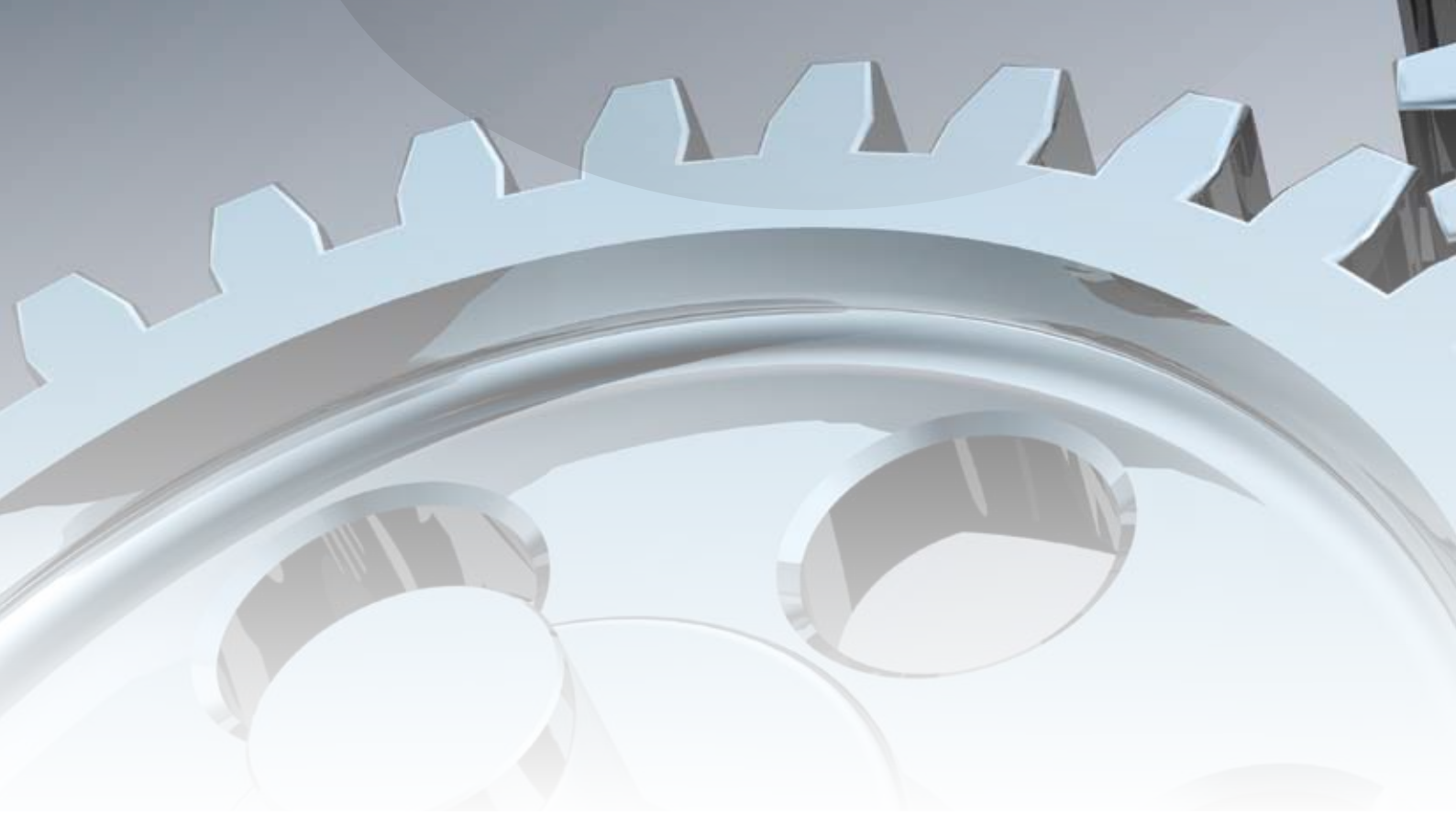
Une fois que le SMCA est mis en œuvre, la norme ISO 22301 exige un suivi permanent ainsi que des réexamens périodiques destinés à améliorer son fonctionnement par :

- un suivi permettant de valider de quelle manière la politique de continuité d'activité de l'organisation a permis d'atteindre les objectifs fixés;
- la mesure de la performance des processus, des procédures et des mesures qui protègent ses activités critiques;
- la surveillance des non-conformités et des déficiences du SMCA;
- la réalisation d'audits internes à intervalles planifiés;
- la surveillance de la conformité à la norme ISO 22301 elle-même ainsi qu'aux objectifs de continuité des activités;
- l'évaluation de tous les éléments précédents dans une revue de direction organisée à intervalles planifiés.

Type d'exercise	Description	Avantages	Désavantages
Liste de contrôle	Distribuer des plans pour revue et réexamen	Assure une revue des activités	N'adresse pas l'efficacité
Walkthrough	Relecture approfondie à chaque étape du plan	Assure que les activités sont décrites avec précision	Faible valeur pour valider l'efficacité
Simulation	Scénario pratique pour valider une partie du plan	Test pratique	Sous-ensemble peut être très différents
Exercice en parallèle	Test complet sans affecter les activités du site primaire	Assure un niveau élevé de fiabilité sans interrompre les opérations normales	Coût élevé
Interruption complète	Test complet par interruption des opérations	Test le plus fiable	Très à risque

|| CLAUSE 10: AMÉLIORATION

L'amélioration continue peut être définie comme l'ensemble des mesures prises dans toute l'organisation pour accroître l'efficacité (atteinte des objectifs) et de l'efficience (un rapport optimal de coût / bénéfice) des processus et des mesures afin d'apporter des avantages accrus pour l'organisation et ses parties prenantes. Une organisation peut améliorer continuellement l'efficacité de son système de gestion grâce à l'utilisation de la politique de continuité des activités, des objectifs, des résultats de l'audit, de l'analyse des événements surveillés, des indicateurs, des actions correctives et préventives et ainsi que d'une revue de direction.



Lien entre ISO 22301 et d'autres standards

ISO 22301 peut être très facilement mis en relations avec d'autres standards en Continuité de l'Activité et en Sécurité de l'Information, comme le récent ISO/IEC 27031:2011 – « Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires ». Publiée en Mars 2011 et remplaçant le standard britannique BS 25777, cette norme internationale décrit les concepts et les principes d'une bonne préparation des TI à la continuité et fournit un référentiel de méthodes et de processus pour identifier et spécifier tous les aspects liés à cette préparation pour améliorer la continuité d'activité.

De la même manière, le SMCA sera également réalisé en pratique à l'aide d'ISO/IEC 24762:2008 – « Lignes directrices pour les services de secours en cas de catastrophe dans les technologies de l'information et des communications ».

Dans les sections suivantes, nous présentons quelques standards avec lesquels ISO 22301 peut être mis en relation afin de créer un système de management intégré.

Lien avec d'autres Système de management de la continuité d'activité

En plus de la norme ISO 22301, on dénombre plusieurs autres standards bien connus, incluant:

- British Standards Institute: BS 25999, Parts 1 and 2
- National Fire Protection Association: NFPA 1600:2010
- ASIS International: ASIS SPC.1-2009
- Standard Australo-Néo-Zélandais: AS/NZS 5050
- Standard Singapourien: SS540
- Standard Canadien: CSA Z1600
- Lignes directrices du PCA du Gouvernement du Japon
- Code des Sociétés Japonaises – PCA
- National Association of Stock Dealers: NASD 3510/3520
- National Institute of Standards and Technology: NIST SP 800-34
- Bourse de New York: NYSE Rule 446

Dans le tableau ci-dessous, la colonne de gauche liste les composants usuels que chaque norme propose, peu ou prou. Les autres colonnes décrivent pour chaque standard où peut être retrouvée l'information pour chaque catégorie. Ce tableau ne fournit pas de détails, ni n'indique le niveau d'utilité de chacune des normes, mais souligne juste le fait que les informations peuvent être retrouvées dans telle ou telle norme.

Elément du SMCA	ISO 22301	ASIS/BSI BCM.01-2010 ASIS	SPC.1:2009 BS	BS 25999:2	NFPA 1600:2010
Compréhension de l'organisation	Section 4.1	N/A	N/A	Section 4.1	N/A
Besoins et attentes des parties intéressées	Section 4.1	N/A	N/A	Section 4.1	Chapitre 4.5
Périmètre	Section 4.3	Section 1	Section 1	Section 3.2.1	Chapitre 5.3
SMCA	Section 4.4	Section 4	Section 4	Section 3	Annex D
Implication de la Direction	Section 5.2	Not explicit	Not explicit	Not explicit	Chapitre 4.1
Politiques	Section 5.3	Section 4.3	Section 4.2.1	Section 3.2.2	Chapitre 4
Rôles et Responsabilités	Section 5.4	Section 4.5.2	Section 4.4.1	Section 3.2.4	Chapitre 6.6
Planification	Section 6	Section 4.4	Section 4.3	Section 3	Chapitre 5
Ressources	Section 7.1	Section 4.5.1	Section 4.4.1	Section 4.3	Chapitre6.1
Compétences	Section 7.2	Section 4.5.3	Section 4.4.2	Section 3.2.4	Chapitre 6.11
Sensibilisation	Section 7.3	Section 4.5.3	Section 4.4.2	Section 3.2.4	Chapitre 6.11
Communication	Section 7.4	Section 4.5.7	Section 4.4.3	Section 4.3.3	Chapitre 6.8
Documentation	Section 7.5	Section 4.6.4	Section 4.5.4	Section 3.4.2	Chapitre 4.8
Analyse d'Impact Métier (BIA)	Section 8.2.2	Section 4.4.1.1	Section 4.3.1	Section 4.4.1	Chapitre 5.5
Analyse de Risque	Section 8.2.3	Section 4.4.1.2	Section 4.3.1	Section 4.1.2	Chapitre 5.4
Stratégies CA	Section 8.3	Section 4.3	Section 4.2	Section 4.2	Chapitre 5
Procédure de Continuité de l'Activité	Section 8.4	Section 4.5.6.2	Section 4.3	Section 4.3.3	Chapitre 6.7
Tests et Exercices	Section 8.5	Section 4.6.2.2	Section 4.5.2.2	Section 4.4	Chapitre 7
Surveillance et Mesurage	Section 9.1	Section 4.6.1	Section 4.5.1	Section 4.4	Chapitre 7.1
Audit interne	Section 9.2	Section 4.6.5	Section 4.5.5	Section 5.1	Chapitre 8.1
Revue de Direction	Section 9.3	Section 4.7.4	Section 4.6.5	Section 5.2	N/A
Amélioration	Section 10	Section 4.7.4	Section 4.6.5	Section 6.2	Chapitre 8
Auditing	Section 9.2	Section 4.6.5	Section 4.5.5	Section 5.1	Chapitre 8.1
Continuous Improvement	Section 10.2	Section 4.7.4	Section 4.6.5	Section 6.2	Chapitre 8

Toutes ces normes de continuité des activités se conforment à l'esquisse commune présentée dans le tableau ci-dessus. Est-ce que cela signifie en fait qu'elles sont identiques? Bien sûr que non mais cela signifie vraiment que toutes celles-ci, à commencer par la norme ISO 22301, répondent aux questions fréquemment rencontrées par chacun des systèmes de management de la continuité de l'activité. C'est pourquoi le système de management qui vient d'être publié pourrait rapidement devenir le standard de prédilection pour les entreprises, ou peut-être même la norme ultime dictée par les réglementations en vigueur dans l'industrie.

Lien avec ISO 27001

ISO 22301 est évidemment directement utile dans le cadre d'un processus de certification à la norme ISO/IEC 27001:2005 par le fait que l'entreprise se conformera ainsi de fait à l'objectif de sécurité des TI de l'article 14 de l'annexe A (Gestion de la Continuité d'Activité). En outre, en ce qui concerne la mise en œuvre et l'exécution d'une BIA dans le cadre du SMSI, elle pourra toujours se référer à la norme ISO/IEC 27005:2011 ou, dans un contexte plus large, à la norme ISO 31000:2009 – « Management du risque - Principes et lignes directrices » ou, pour exécuter l'évaluation elle-même, à la norme ISO 31010:2009 – « Management du risque - Techniques d'évaluation des risques ».

			ISO 22301 Exigences
A.14.1 Gestion de la continuité de l'activité d'un point de vue aspects de la securité de l'information Objectiv: Empécher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les défaillances de systémes d'information ou par des sinistres et garantir une resprise de ces processus dant les meilleurs délais.			**4.4** Système de management de la continuité de l'activité
A.14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de contunuité de factivité	*Mesure* Un processus de continuité de l'activité dans l'ensemble de l'organisme doit étre élaboré et géré, qui satisfait aux exigences en matiére de sécurité de l'information requises pour la continuité de l'activite de l'organisme	**8.2** BIA and Risk assessment
A.14.1.2	Contunuité de l'activité et appréciation du risque	*Mesure* Les événements pouvant étre á l'orgine d'interruptions des processus métier doivent étre identifiés, tout comme ia probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.	
A.14.1.3	laboration et mise en ceuvre de plans de continuité intégrant la sécurité de l'information	*Mesure* Des plans doivent étre élaborés et mis en ceuvre pour maintenir ou restauer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite á une interruption ou une panne affectant les processus métier cruciaux.	**8.4** Procédures de continuité de l'activités
A.14.1.4	Cadre de la planification de la contiunité de l'activité	*Mesure* Un cadre unique pour les plans de continuité de l'activité doit étre géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de maniére constante aux exigences en matiére de sécurité de l'information et d'identifier les priorités en matiére de mise á l'essai et de maintenance.	**6** Planification du SMCA
A.14.1.5	Mse á l'essai, gestion et réévauation, constante des plans de continuité de factivité	*Mesure* Les plans de continuité de l'activité de l'activite doivent étre testés et mis á jour réguliérement afin de s'assurer qu'ils sont actulisés et efficaces.	**8.5** Exercices et tests

Intégration avec d'autres systèmes de management

Les exigences générales présentées dans le tableau ci-dessous sont couramment indiquées dans tout système de management. Elles se rapportent à la fixation des objectifs, en les adaptant aux habitudes de fonctionnement et aux besoins de l'organisation. Ces exigences permettent de garantir le fait de pérenniser les objectifs en se basant sur un engagement de solide de la Direction ; elles assurent la mise en place d'une surveillance et d'un soutien du système de management à travers une documentation fiable. Elles imposent des contrôles de l'état de santé du système à intervalles réguliers par l'intermédiaire d'audits internes ou externes et permettent de recueillir des bénéfices à travers l'amélioration continue notamment via des revues de direction régulières.

Le tableau ci-dessous montre comment un SMCA peut être considéré en combinaison avec d'autres systèmes de management. Ceci doit permettre à toute organisation d'envisager des audits « joints » ou « combinés » leur permettant d'atteindre leurs objectifs de conformité moyennant un effort et un budget intégrés.

Exigences	I ISO 9001:2008	ISO 14001:2004	ISO 20000:2011	ISO 22301:2012	ISO 27001:2005
Objectifs du système de management	5.4.1	4.3.3	4.5.2	6.2	4.2.1
Politique du système de management	5.3	4. 2	4.1.2	5.3	4.2.1
Engagement de la direction	5.1	4.4.1	4.1	5.2	5
Exigences relatives à la documentation	4.2	4.4	4.3	7.5	4.3
Audit interne	8.2.2	4.5.5	4.5.4.2	9.2	5
Amélioration continue	8.5.1	4.5.3	4.5.5	10	8
Revue de direction	5.6	4.6	4.5.4.3	9.3	7

Management de la Continuité de l'Activité – Principaux Bénéfices

Comme lors de tout grand chantier au sein d'une organisation, il est essentiel d'obtenir le soutien et le parrainage de la Direction. Le meilleur moyen d'y parvenir, et de loin, consiste à illustrer le gain majeur que représente le fait de disposer d'un processus de management de la continuité de l'activité plutôt que d'aborder le sujet en soulignant uniquement les aspects négatifs de l'interruption d'activité.

Aujourd'hui, une bonne gestion de la continuité de l'activité ne consiste pas simplement à prendre des mesures pour faire face aux pressions externes. Il s'agit de reconnaître la valeur positive de la bonne pratique de continuité des opérations forgée au sein même de l'organisation.

Réaction prévisible et efficace en cas de crise	**Protection des personnes**	**Maintien des activités vitales de l'organisation**	**Meilleure compréhension de l'organisation**
Réduction de coûts	**Respect de la communauté et des parties prenantes**	**Protection de la réputation et de la marque de commerce**	**Confiance des clients**
Avantage concurrentiel	**Conformité légale**	**Conformité réglementaire**	**Conformité contractuelle**

L'adoption d'un processus de Management de la Continuité de l'Activité efficace au sein d'une organisation présentera des avantages dans un certain nombre de domaines, dont, par exemple:

1. Protection de la valeur actionnariale
2. Réduction de l'exposition à des risques spécifiques à travers une identification méthodique du risque
3. Compréhension améliorée du métier obtenue durant l'analyse de risque
4. Résilience opérationnelle résultant de la réduction du risque
5. Réduction du temps d'arrêt lorsque des processus alternatifs et des contournements sont identifiés
6. Problèmes de conformité identifies et gérés pour les processus alternatifs
7. Enregistrements vitaux qui peuvent être maintenus et protégés
8. Les implications en matière de législation « Santé & Sécurité » et les devoirs de bonne diligence qui peuvent être correctement considérés
9. Efficacité opérationnelle améliorée à travers un programme imposé de réingénierie des processus métiers
10. Meilleure résilience organisationnelle par la désignation de personnel alternatif pour supporter les processus clés et par la définition et la documentation des processus de restauration
11. Protection des actifs physiques et informationnels du métier
12. Préservation des marchés par l'assurance de la continuité de l'approvisionnement
13. Amélioration globale de la sécurité
14. Prévention d'actions en responsabilité

Mise en œuvre d'un SMCA avec la méthode IMS2

Prendre la décision de mettre en œuvre un Système de Management de la Continuité de l'Activité basé sur ISO 22301 est souvent relativement simple dans la mesure où les bénéfices en sont assez explicites. La plupart des entreprises constatent maintenant qu'il n'est pas suffisant de simplement mettre en place un Plan de Continuité générique "muti-usages". Pour assurer une réponse efficace, dans le cadre du maintien de la continuité opérationnelle, ce plan doit être personnalisé eu égard à des risques spécifiques et à des scénarios catastrophiques qui peuvent s'échelonner de la perte d'un immeuble entier jusqu'à l'interruption de systèmes très localisés. Une tâche bien plus difficile consiste alors corréler les divers plans et à les compléter dans une perspective qui respecte les exigences du standard, les besoins métier et les échéances avant la certification.

Il n'existe pas de plan type pour mettre en œuvre ISO 22301 qui puisse s'appliquer indifféremment à toutes les entreprises mais il y a des étapes communes qui permettront à chaque organisation de trouver un bon équilibre entre des exigences parfois contradictoires et lui permettront à se préparer à la réussite d'un audit de certification.

PECB a développé une approche et une méthode pour mettre en œuvre un système de management, appelée "Integrated Implementation Methodology for Management Systems and Standards (IMS2)" et basée sur les meilleurs pratiques applicables. Cette méthode est base sur les lignes directrices des standards ISO et rencontre également les exigences particulières d'ISO 22301.

1. Planifier

- 1.1 Initialiser le SMCA
- 1.2 Compréhension de l'organisme
- 1.3 Analyse du système existant
- 1.4 Leadership et approbation projet
- 1.5 Périmètre
- 1.6 Politique de continuité de l'activité
- 1.7 Analyse d'impacts
- 1.8 Analyse de risque

2. Déployer

- 2.1 Stratégie de continuité
- 2.2 Structure organisationelle
- 2.3 Gestion documentaire
- 2.4 Mesures de protection& mitigation
- 2.5 Plan & procédures de continuité de l'activi
- 2.6 Communication
- 2.7 Formation & sensibilisation
- 2.8 Exercises et test

3. Contrôler

- 3.1 Surveillance mesurage, analyse et Évaluation
- 3.2 Audit interne
- 3.3 Revue de direction

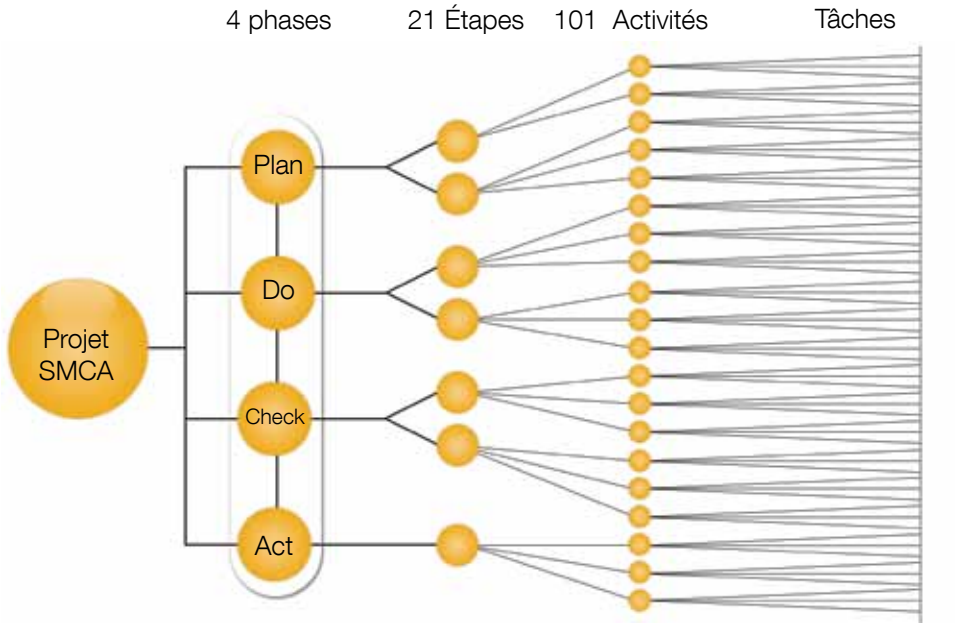
4. Agir

- 4.1 Traitement des nonconformités
- 4.2 Amélioration continue

IMS2 est basé sur le cycle PDCA divisé en quatre phases: Planifier, Déployer, Contrôler et Agir. Chaque phase comprend entre 2 et 8 étapes sur un total de 21 étapes. À leur tour, ces étapes sont divisées en 101 activités et tâches. Ce guide pratique considère les phases-clés de mise en œuvre de votre projet du début à la fin et suggère les meilleures pratiques pour chacun d'eux, en vous dirigeant également vers d'autres ressources utiles qui vous aideront dans votre voyage vers la conformité ISO 22301.

En suivant une méthodologie structurée et efficace, une organisation peut être sûre qu'elle couvre au moins toutes les exigences minimales pour la mise en œuvre d'un système de management. Quelle que soit la méthode utilisée, l'organisation devra l'adapter à son contexte particulier (exigences, taille de l'organisation, périmètre, objectifs, etc...) et ne pas tenter de l'appliquer comme une simple recette de cuisine.

La séquence des étapes peut être modifiée (inversion, fusion). Par exemple, la mise en œuvre de la procédure de gestion de la documentation peut être réalisée avant de posséder une compréhension détaillée de l'organisation. De nombreux procédés sont également itératifs en raison de la nécessité d'un développement progressif tout au long du projet de mise en œuvre, par exemple, la communication et la formation.



Certification des organisations

Le trajet usuel pour une organisation souhaitant se faire certifier envers ISO 22301 est le suivant:

1. Mise en oeuvre du système de management: Avant d'être audité, un système de management doit fonctionner depuis un certain temps. Habituellement, le temps minimum avant un premier audit qui est requis par les organismes de certification est de 3 mois.
2. Audit interne et revue de Direction: Avant qu'un système de management puisse être certifié, il doit avoir fait l'objet d'au moins un audit interne et d'au moins une revue de Direction.
3. Sélection d'un organisme de certification (registraire): Chaque organisation peut sélectionner l'organisme de certification (registraire) de son choix.
4. Audit de pré-évaluation (optionnel): Une organisation peut choisir de réaliser un pré-audit pour identifier les écarts possibles entre son système de management actuel et les exigences de la norme.
5. Audit de phase 1 (Documentaire): Il s'agit d'une revue de la conformité de la conception du système de management. L'objectif principal de cette phase est de vérifier que le système de management est conçu pour rencontrer les exigences de la norme et des objectifs de l'organisation. Il est recommandé qu'au moins une partie de la l'audit de phase 1 soit réalisé sur site dans les locaux de l'organisation auditée.
6. Audit de Phase 2 (Visite sur site): L'objectif de la phase é de l'audit de certification est d'évaluer si le système de management tel que déclaré est conforme aux exigences de la norme et est déployé au sein de l'organisation afin de lui permettre d'atteindre ses objectifs. La phase 2 se déroule sur place, au sein de l'organisation dans laquelle est déployé le système de management.
7. Audit de suivi (optionnel): Si l'organisation auditée fait l'objet de déclarations de non-conformités qui requièrent une visite additionnelle avant certification, l'auditeur réalisera un audit de suivi pour valider uniquement les plans d'action lies aux non conformités (généralement sur une seule journée).
8. Confirmation de l'enregistrement: Si l'organisation est conforme avec les conditions exigées par la norme, le registraire confirme la certification et publie le certificat.
9. Amélioration continue et audits de surveillance: Une fois qu'une organisation est enregistrée, des activités de surveillance sont menées par l'organisme de certification pour assurer que le système de management reste conforme avec les exigences de la norme. Les activités de surveillance doivent inclure des visites sur site (au moins une fois par an) qui permettent de vérifier la conformité du système de management du client et peuvent aussi inclure : des investigations suite à des plaintes, revue d'un site Internet, une requête de suivi écrite, etc.

Formation et certifications de professionnels

PECB a développé une feuille de route pour chefs de projet et auditeurs d'une organisation qui souhaite se faire certifier envers ISO 22301. De la même manière que la certification est un composant vital du secteur de la Sécurité de l'Information puisqu'elle fournit la preuve que les organisations ont développé des comportements standardisés basés sur les meilleures pratiques, la certification individuelle sert de preuve documentée des qualifications professionnelles, des compétences et de l'expérience des personnes qui ont suivi les cours et réussi les examens. Elle démontre que le professionnel certifié détient les compétences définies par les meilleures pratiques. Elle permet aussi aux organisations de réaliser une sélection éclairée des employés ou des services basés sur leurs compétences reprise dans la désignation de la certification. Finalement, elle fournit un incitant à chaque professionnel pour améliorer continuellement ses capacités et ses connaissances et sert d'outil aux employeurs pour assurer que les formations et les sessions de sensibilisation sont efficaces.

Les formations de PECB sont offertes globalement à travers un réseau de centre de formation, accrédités et sont disponibles en plusieurs langues. Elles incluent des sessions d'introduction, les fondements des différentes normes, la gestion du déploiement (gestion de projet) et l'audit de systèmes de management. Le tableau ci-dessous donne une brève description des cours officiels de PECB pour ce qui concerne les systèmes de management de la continuité de l'activité basés sur ISO 22301.

Titre de la formation	Résumé	À qui s'adresse la formation
Introduction à ISO 22301	• Formation d'une journée • Introduction aux concepts de gestion et de déploiement d'un SMCA • Ne conduit pas à une certification	• Professionnels des TI • Equipe impliquée dans le déploiement d'un SMCA • Consultants ICT • Managers responsible du déploiement d'un SMCA • Auditeurs
Fondements d'ISO 22301	• Formation de 2 jours • Se familiariser avec les meilleures pratiques pour le déploiement et la gestion d'un SMCA • Examen d'une heure	• Membres d'une équipe de continuité d'activité • Professionnels des TI • Equipe impliquée dans un SMCA • Techniciens • Auditeurs
ISO 22301 Lead Implementer	• Formation de 5 jours • Gérer le déploiement et assurer les operations d'un SMCA • Examen de 3 heures	• Project managers et/ou consultants • Auditeurs en continuité d'activité • Membres d'une équipe de continuité d'activité • Experts techniques
ISO 22301 Lead Auditor	• Formation de 5 jours • Gérer l'audit d'un SMCA • Examen de 3 heures	• Auditeurs internes • Auditeurs • Project managers et/ou consultants • Membres d'une équipe de continuité d'activité • Experts techniques

Aucun programmes d'étude particulier n'est nécessaire dans le cadre du processus de certification. Pour autant, la réussite d'un cours PECB reconnu ou d'un programme d'étude améliorera considérablement vos chances de réussite d'un examen de certification PECB. Vous pouvez vérifier la liste des organismes reconnus qui offrent des sessions de formation de PECB officiels sur notre site Web sur www.pecb.org/fr/EventList.

|| choix de la certification droit

La certification « Fondements d'ISO 22301 » est une certification destinée aux professionnels qui ont besoin d'acquérir une compréhension globale de la norme ISO 22301 et de ses exigences.

La certification « ISO 22301 Implementer » est une certification destinée aux professionnels qui ont besoin de mettre en œuvre un Système de Management de la Continuité de l'Activité (SMCA) et, dans cas de la certification « ISO 22301 Lead Implementer », qui doivent savoir gérer un projet de déploiement.

La certification « ISO 22301 Auditeur » est une certification destinée aux professionnels qui doivent pouvoir auditer un Système de Management de la Continuité de l'Activité (SMCA) et, dans le cas de la certification "ISO 22301 Lead Auditor", qui doivent savoir gérer une équipe d'auditeurs.

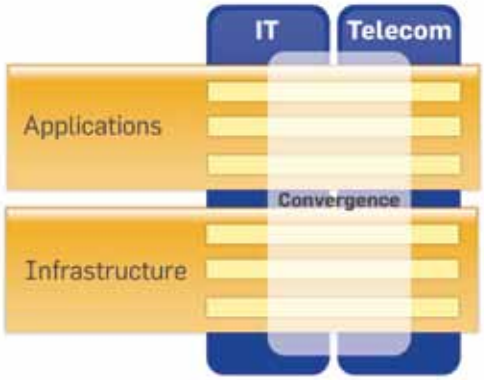
La certification « ISO 22301 Master » est une certification destinée aux professionnels qui doivent à la fois maîtriser les aspects de déploiement d'un Système de Management de la Continuité de l'Activité (SMCA) et de maîtriser les techniques d'audit ainsi que de gérer (ou participer à) des équipes et des programmes d'audit.

Sur la base de votre expérience professionnelle globale et des qualifications que vous avez acquises, vous serez certifié sur un ou plusieurs de ces schémas de certifications sur base de projets ou d'activités d'audit que vous avez mené par le passé ou sur lesquels vous êtes occupés au moment de votre demande de certification.

Désignation professionnelle	Examen	Expérience professionnelle	Expérience d'Audit	Expérience de projet
ISO 22301 Provisional Auditor	ISO 22301 Lead Auditor	Aucune	Aucune	Aucune
ISO 22301 Auditor	ISO 22301 Lead Auditor	2 années (1 en continuité d'activité)	200 heures	Aucune
ISO 22301 Lead Auditor	ISO 22301 Lead Auditor	5 années (2 en continuité d'activité)	300 heures	Aucune
ISO 22301 Provisional Implementer	ISO 22301 Lead Implementer	Aucune	Aucune	Aucune
ISO 22301 Implementer	ISO 22301 Lead Implementer	2 années (1 en continuité d'activité)	Aucune	200 heures
ISO 22301 Lead Implementer	ISO 22301 Lead Implementer	5 années (2 en continuité d'activité)	Aucune	300 heures
ISO 22301 Master	ISO 22301 Lead Implementer ISO 22301 Lead Auditor	10 années (6 en continuité d'activité)	500 heures	500 heures

About DEVOTEAM

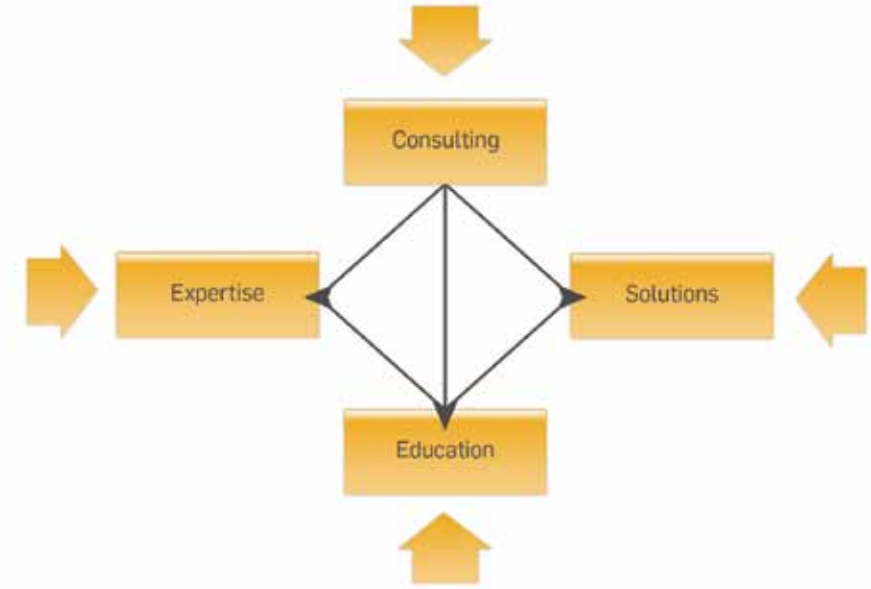
Devoteam NV/SA is a leading ICT service company with a very solid knowledge base of more than 260 highly skilled experts in Belgium and an international network of more than 4500 colleagues in the Devoteam Group.
Thanks to its genes, **Devoteam NV/SA has a very strong background in IT, Telecommunication and Media realizations.** Devoteam offers **solutions** and **services** covering IT and Telecom in the two specific domains of applications and infrastructure.



Applications:
- Enterprise Content Management
- Applications for Digital Television
- Business Application Integration

Infrastructure:
- IT Service Management
- Advanced Infrastructure Services
- Risk & Security Management

Depending on customer's needs, Devoteam NV/SA in Belgium can offer its experience through **consultancy, expertise, education** as well as by providing complete **solutions**. Devoteam NV/SA has a long experience in doing projects and quality assurance. Devoteam has several Prince2 certified project managers and an ISO 9001:2008 certificate.



Excellence. Compétence. Reconnaissance

EXCELLENCE.
COMPÉTENCE.
RECONNAISSANCE.

PECB – Professional Evalution and Certification Board

7275 Sherbrooke East, Suite 32
CP 49060, Montreal, QC
H1N 1H0, CANADA

80 Broad Street, 5th Floor
New York City, NY
10004, USA

Email:

General inquiries: info@pecb.org
Certification: certification@pecb.org
Examens Training: examination@pecb.org
Formation: training@pecb.org
Support technique: support@pecb.org

Tel: 1-514-562-5464
Fax: (202) 618-6264

www.pecb.org