



Chambre Professionnelle
du Conseil
LANGUEDOC-ROUSSILLON

KEYNOTE
JOURNÉE DU CONSEIL
Le 11-06-20

Certification ISO27001

Systeme de Management de la
Sécurité de l'Information SMSI



Le contenu de ce support est la propriété de PDCA
Consultant
0776884650, 5 rue des Poiriers 34090
MONTPELLIER, contact@pdca-consultant.fr

Toute utilisation ou modification nécessite
l'autorisation de ce dernier

Journée du Conseil – 11 juin 2020





PROGRAMME

- Introduction (présentation PDCA Consultant)
- Les systèmes de Management
- La famille des normes ISO27000
- La structure de la norme ISO27001
- La sécurité de l'information
- Pourquoi s'engager dans la démarche ?
- Comment mettre en place un SMSI ?
- Démarche de certification
- Pour aller plus loin...

Mais pour **VOUS**...

C'est quoi Un Système de Management ?

- Système permettant d'établir une politique
- D'établir des objectifs
- D'atteindre ces objectifs





Les systèmes de management de la sécurité de l'information

C'est un ensemble de mesures
organisationnelles et techniques visant à
atteindre un objectif et une fois celui-ci atteint,
à s'y tenir

**PAS
MOINS**



PAS PLUS

PROPRIETES DES SYSTEMES DE MANAGEMENT

Large spectre de métiers et de
compétences
(Approche processus)

Un projet fédérateur
et mobilisateur
(tous concernés)

Importance de l'écrit
(Traçabilité)

Auditabilité
(processus d'audit)



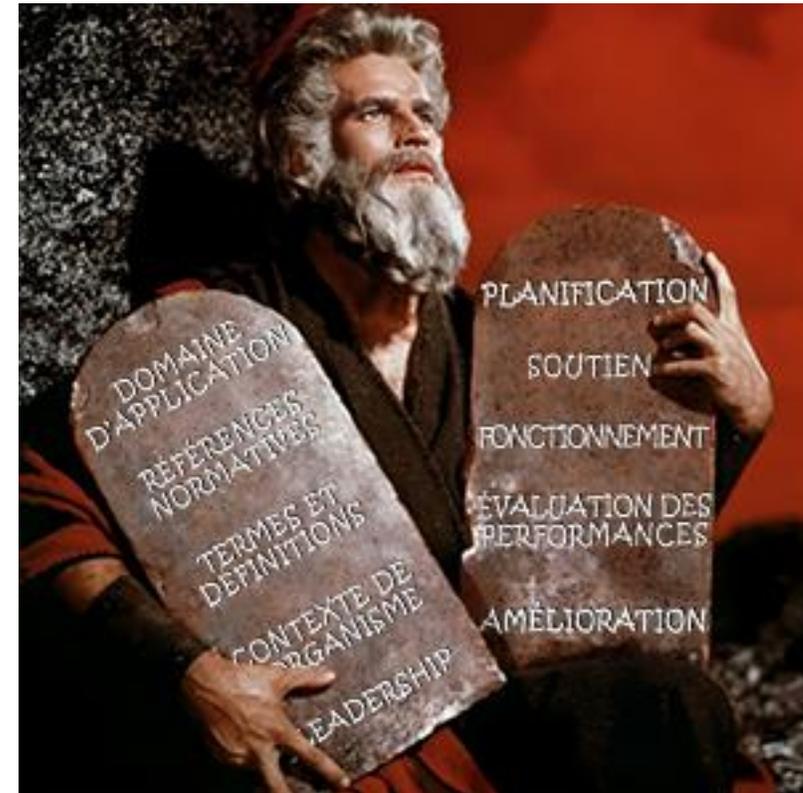
Les Principaux Systèmes de Management (France) source ISO-SURVEY 2018

SYST. De Management	REFERENTIEL	Nbre certificats	Nbre sites
QUALITE	ISO9001:2015	21095	58467
ENVIRONNEMENT	ISO14001:2015	6084	19468
DISPOSITIF MEDICAUX	ISO13485:2016	1102	1716
ENERGIE	ISO50001:2018	770	7703
SECURITE de l'INFORMATION	ISO27001:2017	223	925
SECURITE ALIMENTAIRE	ISO22000:2018	140	154
SANTE-SECURITE	ISO45001:2018	94	208



STRUCTURE dite « HLS » (HIGH LEVEL STRUCTURE)

- * Identique à tous les systèmes de management
- * Superposables
- * Non contradictoires
- * Audits intégrés





La structure de la norme ISO27001

Chap.0 : Introduction

Chap. 1: Domaine d'application

Chap. 2: Références normatives

Chap. 3: Termes et définitions

P = Plan
(établir)

Chap. 4: contexte de l'organisation
Chap. 5: Leadership
Chap.6: Planification
Chap. 7: Support

D = Do
(implémenter)

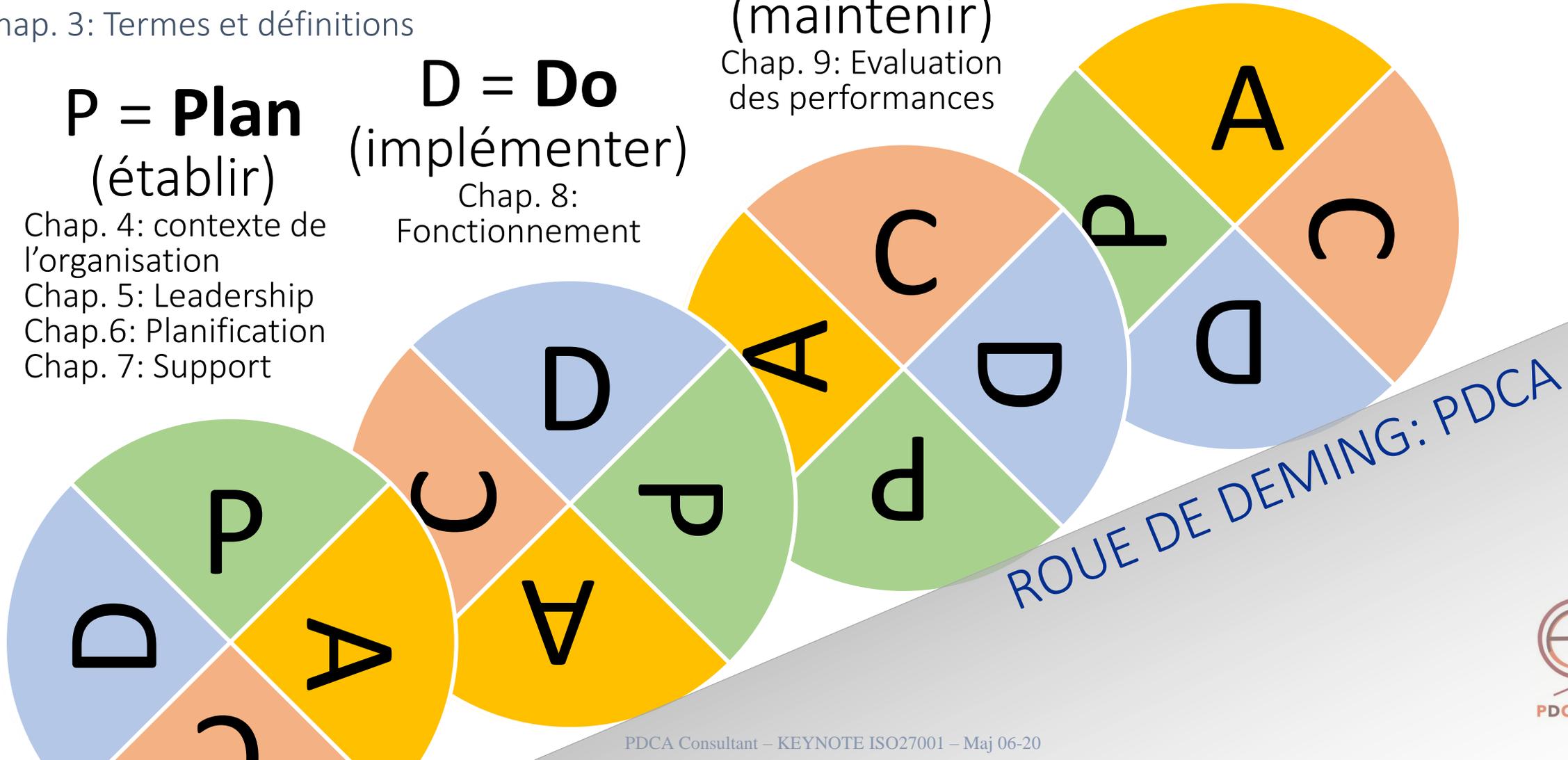
Chap. 8:
Fonctionnement

C = Check
(maintenir)

Chap. 9: Evaluation des performances

A = Act
(améliorer)

Chap. 10:
Amélioration



et en PLUS....

une ANNEXE A (NORMATIVE)

- Sous forme de tableau décrivant 114 objectifs et mesures
- Permettant de répondre aux exigences de l'article 6.1.3: traitement des risques de sécurité de l'information
- Permettant à chaque organisme de s'assurer qu'aucune mesure n'a été omise, ce qui entraîne une déclaration d'applicabilité



Exemple: Appareils mobiles et télétravail

- A.6.2: Assurer la sécurité du télétravail et de l'utilisation des appareils mobiles
- A.6.2.1: Une politique et des mesures de sécurité complémentaire doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles
- A.6.2.2: Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail





Que signifie Sécurité de l'information ?





SECURITE DE L'INFORMATION

Quand on dit « sécurité de l'information.... »
→ Cela ne veut pas uniquement dire sécurité informatique

Il s'agit de l'**INFORMATION** sous toutes ses formes :

- logiciel
- matériel
- humain
- papier
- Savoir-faire
- Etc.



Le mot « **SECURITE** » désigne...

→ Tout de qui peut avoir des conséquences (négatives ou positives) en matière :

- De confidentialité
- De disponibilité
- Ou d'intégrité de l'information.

- **La norme n'impose pas de niveau minimum de sécurité à atteindre dans le SMSI. Son niveau devant être proportionné aux risques évalués.**

OBJECTIFS PRINCIPAUX D'UN S.M.S.I = PRESERVER CES 3 PROPRIETES POUR LES INFORMATIONS LES PLUS SENSIBLES DE L'ORGANISME



SECURITE DE L'INFORMATION

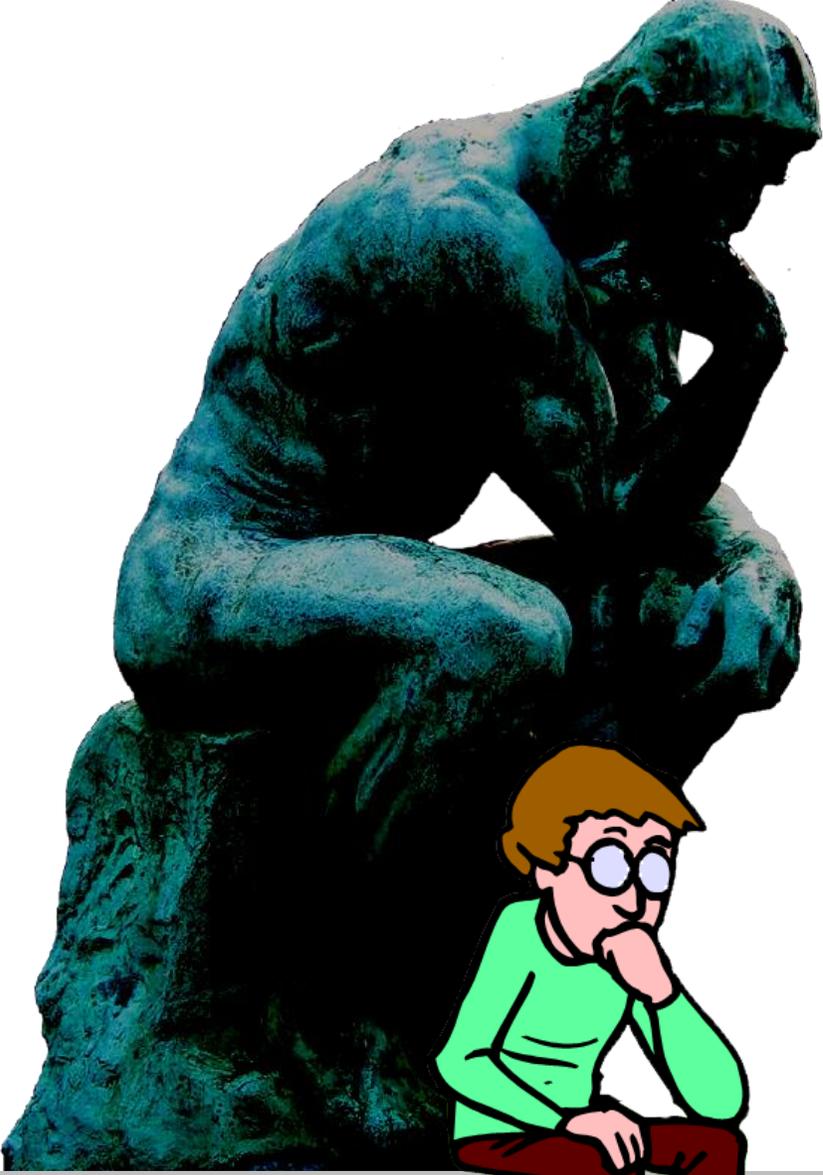
CONFIDENTIALITE: l'information ne doit pas être divulguée à toute personne, identité ou processus non autorisé

INTEGRITE: le caractère correct et complet des actifs doit être préservé

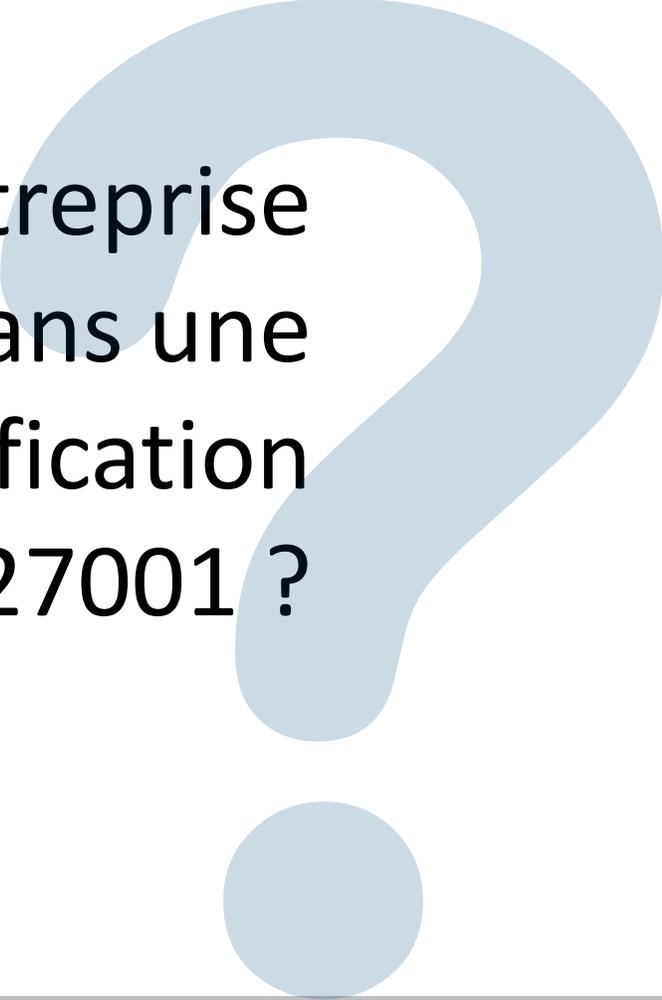
DISPONIBILITE: L'information doit être rendue accessible et utilisable sur demande par une entité autorisée

ATTENTION: exigence de **CONTINUITE** de la sécurité de l'information





Pourquoi une entreprise
s'engage-t-elle dans une
démarche de certification
ISO27001 ?



Le chef d'entreprise

GLOUPS !



*Je compte
sur vous pour que vous
soyez bientôt certifié...*

Pourquoi une
s'engage-t-elle dans une
démarche de certification
ISO27001 ?

Parce que
le client
le lui
demande

Le chef d'entreprise

COMMENT REDUIRE
LES RISQUES LIES AU
SI ?

COMMENT
AMELIORER LA
COMPETITIVITE ?

COMMENT RÉDUIRE
LA PROBABILITE
D'ERREUR TIC ?

COMMENT
AUGMENTER LA
CONFIANCE ?

COMMENT ETRE
CONFORME A LA
REGLEMENTATION ?

COMMENT
PROTEGER
L'ORGANISATION ?

Pour s'engager dans une démarche de certification ISO27001 ?

Parce que
la démarche
répond à un besoin
d'organisation...



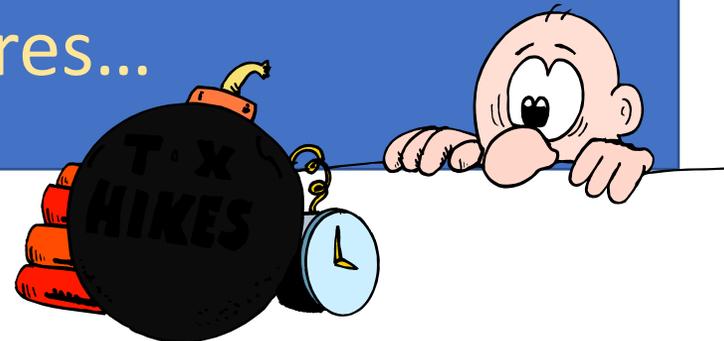
PDCA Consultant



Pourquoi une entreprise
s'engage-t-elle dans une
démarche de certification

ISO27001 ?

Parce l'entreprise doit faire face
à des risques... économiques, financiers,
techniques, réglementaires, sociaux,
concurrentiels, sanitaires...



Comment mettre en place un SMSI?





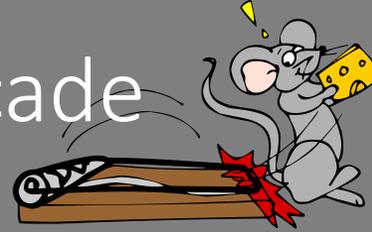
Clés de la réussite et pièges à éviter

L'usine à gaz



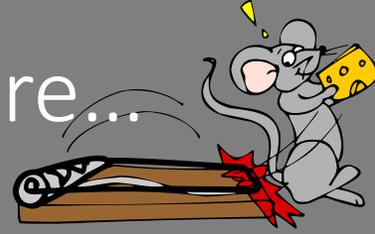
Si c'est trop
compliqué,
le système aura
du mal à vivre





Construire un système utile

La cathédrale documentaire...



CA Y EST, J'AI
RETROUVÉ LA
PROCÉDURE...



Ne formaliser
que si cela présente
un risque





Implication de tous... et de chacun

Le Manager d'abord
(Leadership)

N'oublier personne





Réactivité

Se donner le temps de réussir la démarche



PDCA Consultant



Communication

Expliquer de manière compréhensible pour
tous

les objectifs, le rôle de chacun et les résultats

EN
PARLANT FORT
ON S'ENTEND
MIEUX !

IL Y A
D'AUTRES
MÉTHODES
PLUS SOFT...





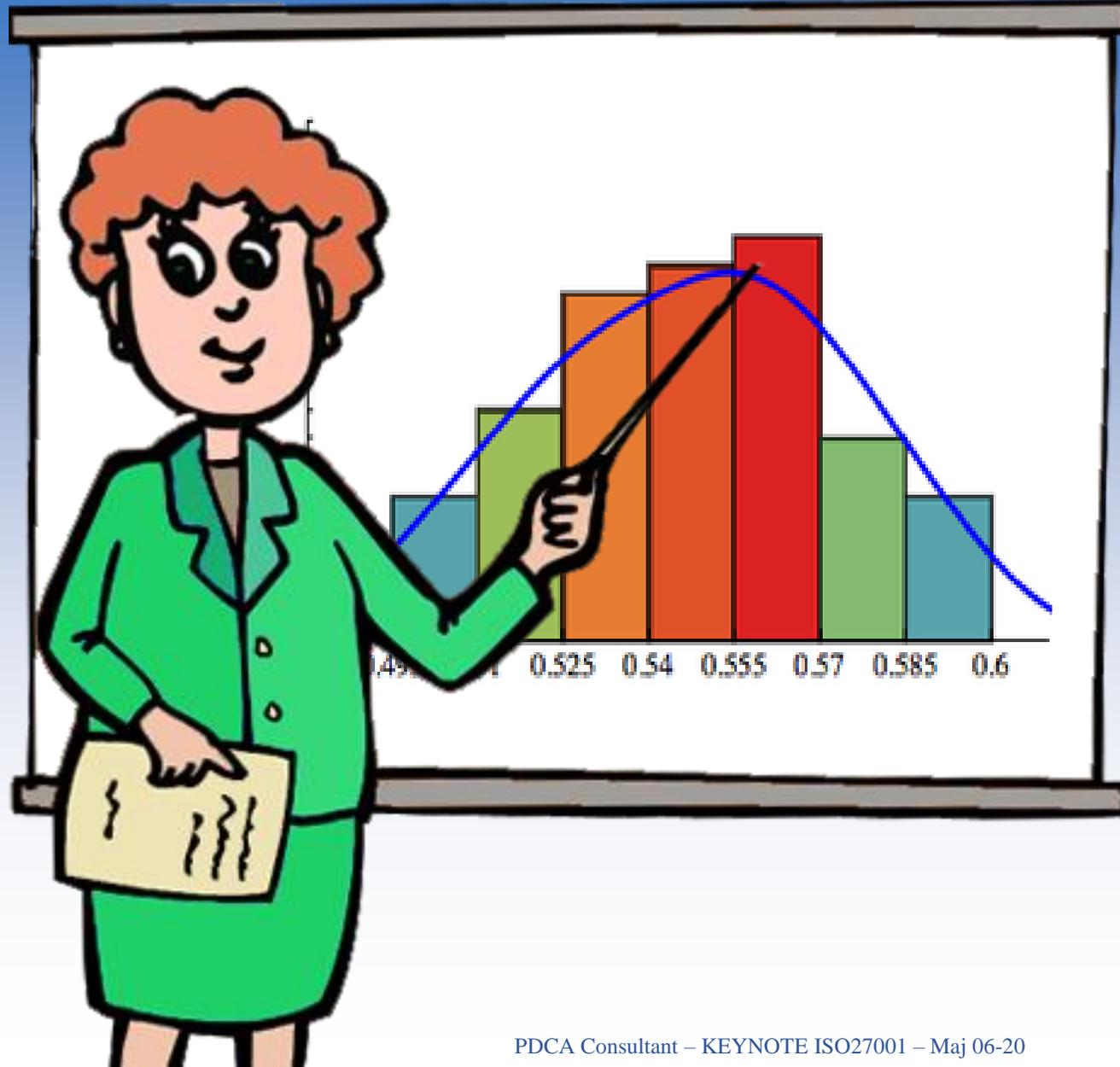
Utilisation des acquis

Ne pas tout remettre en cause : l'entreprise existe...
(l'eau chaude aussi)





Décision

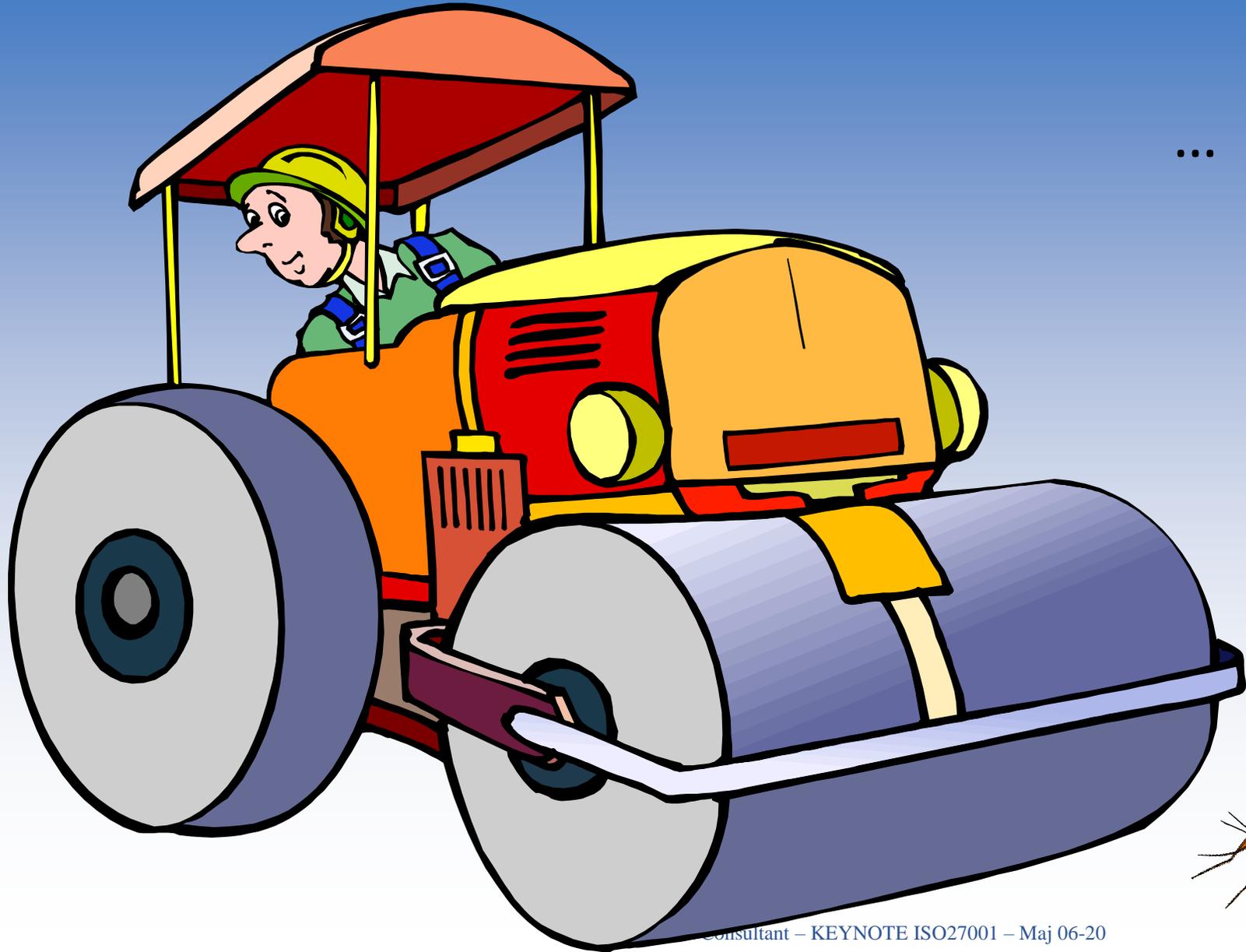


Prendre
les décisions
en s'appuyant
sur les
résultats





Et surtout...

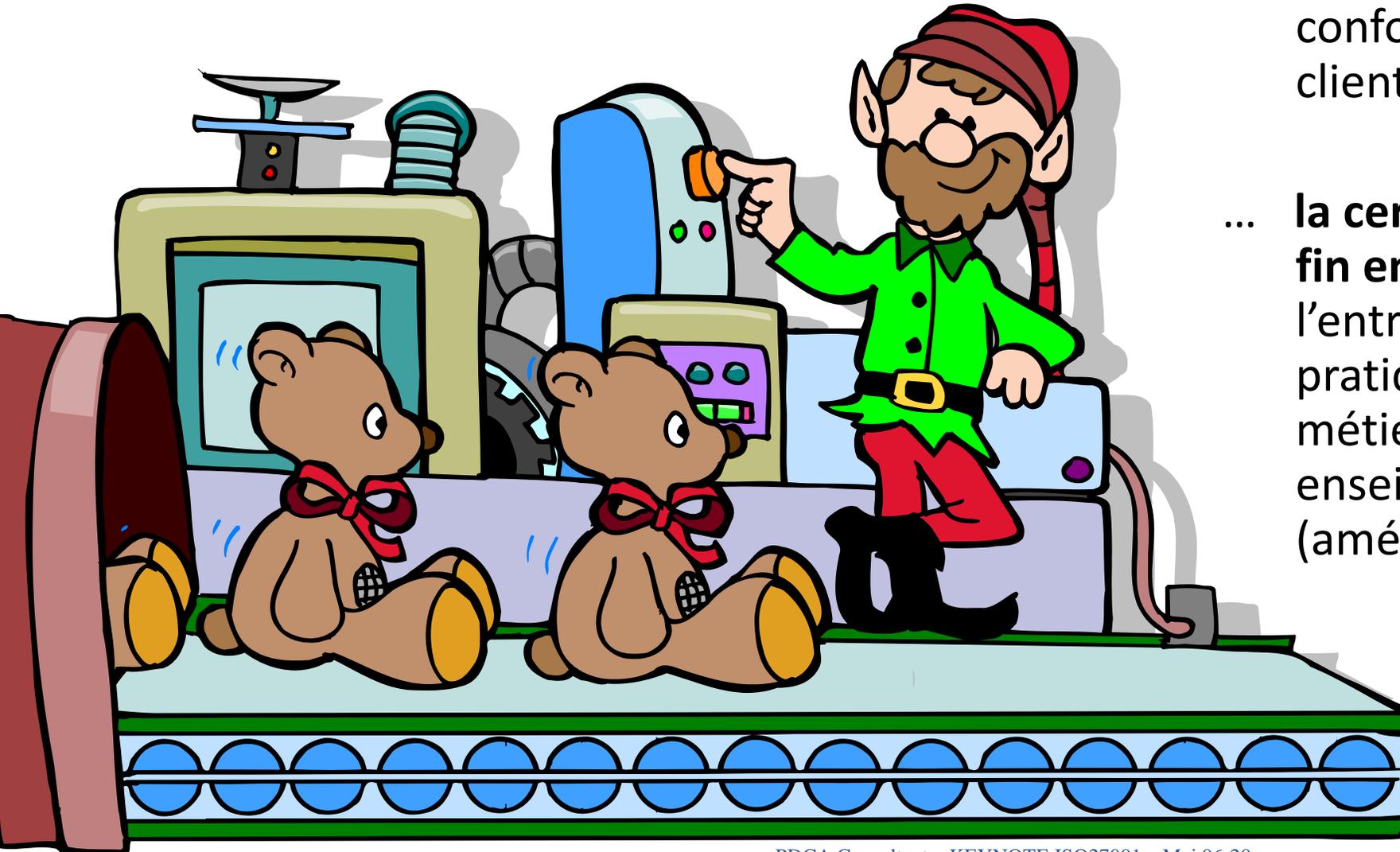


... la démarche doit rester proportionnelle à la taille de l'entreprise et à ses enjeux.



PDCA Consultant

Ne perdons pas de vue que...



... **le métier de l'entreprise** reste la fabrication d'un produit ou la réalisation d'un service conforme aux exigences des clients (et réglementaires)

... **la certification n'est pas une fin en soi**, mais un moyen pour l'entreprise de s'organiser pour pratiquer efficacement son métier, et de tirer les enseignements de ses erreurs (amélioration continue)

Et aussi... une entreprise doit être pérenne et **créer de la valeur**



**La mise en œuvre efficace
d'un S.M.S.I. basé sur
le référentiel ISO 27001
peut générer du profit...**

LES

FONDAMENTAUX

de la **PERFORMANCE**
(EFFICACITÉ et EFFICIENCE)



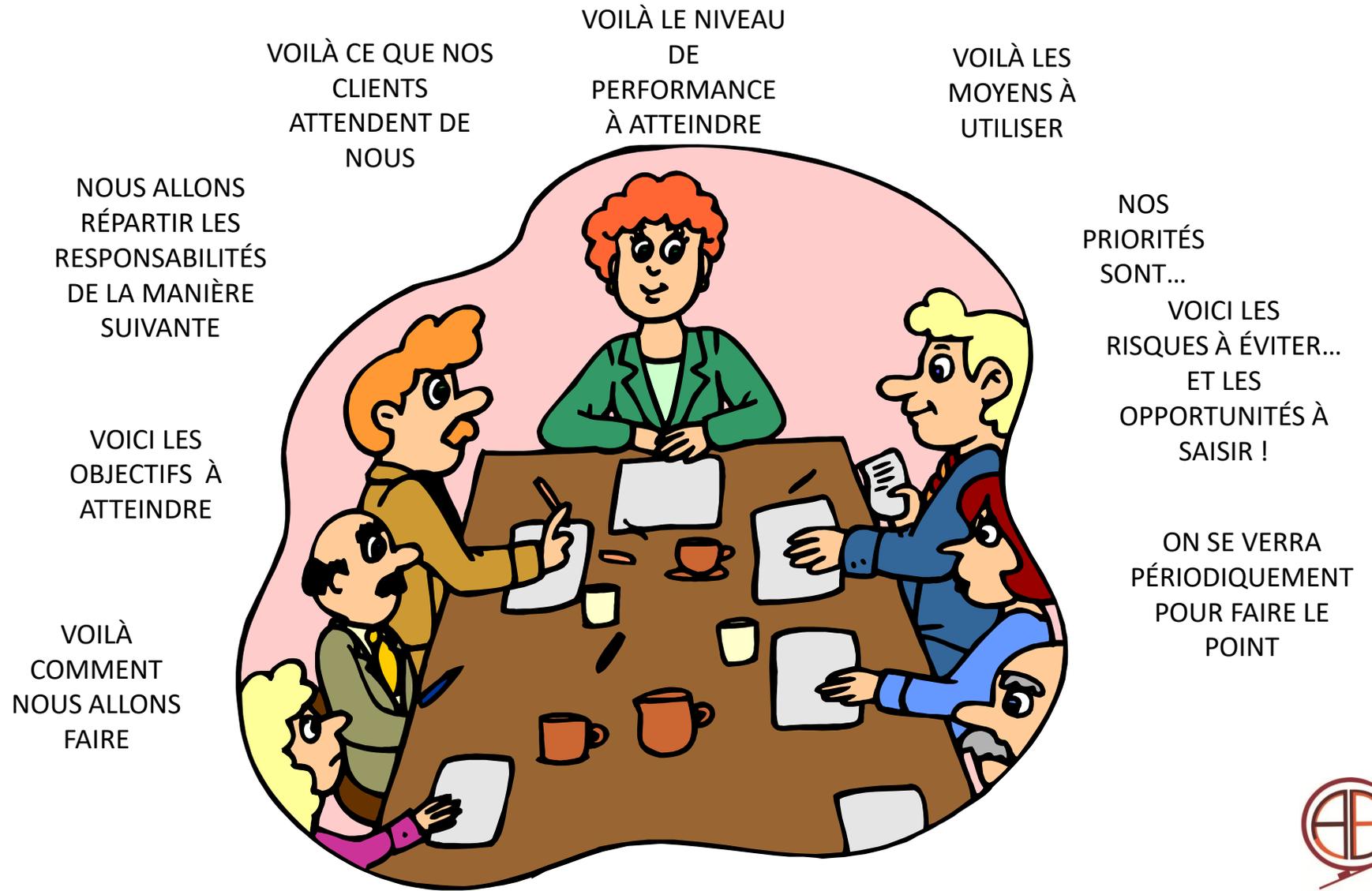
Les 7 fondamentaux de la performance

ORIENTATION CLIENT



Les 7 fondamentaux de la performance

LEADERSHIP:
*obligation de diligence
de la direction*



Les 7 fondamentaux de la performance

LORS D'ENTRETIENS AVEC LES PERSONNELS NOUS IDENTIFIONS LEURS BESOINS EN FORMATION ET EN MESURONS L'EFFICACITE

POUR QUE MON ENTREPRISE FONCTIONNE, JE M'ENTOURE DE GENS COMPÉTENTS ET MOTIVÉS (phase de pré-
embauche)

SI J'AI DES LACUNES, MON PATRON FAIT LE NÉCESSAIRE

JE SAIS CE QUE MON PATRON ATTEND DE MOI

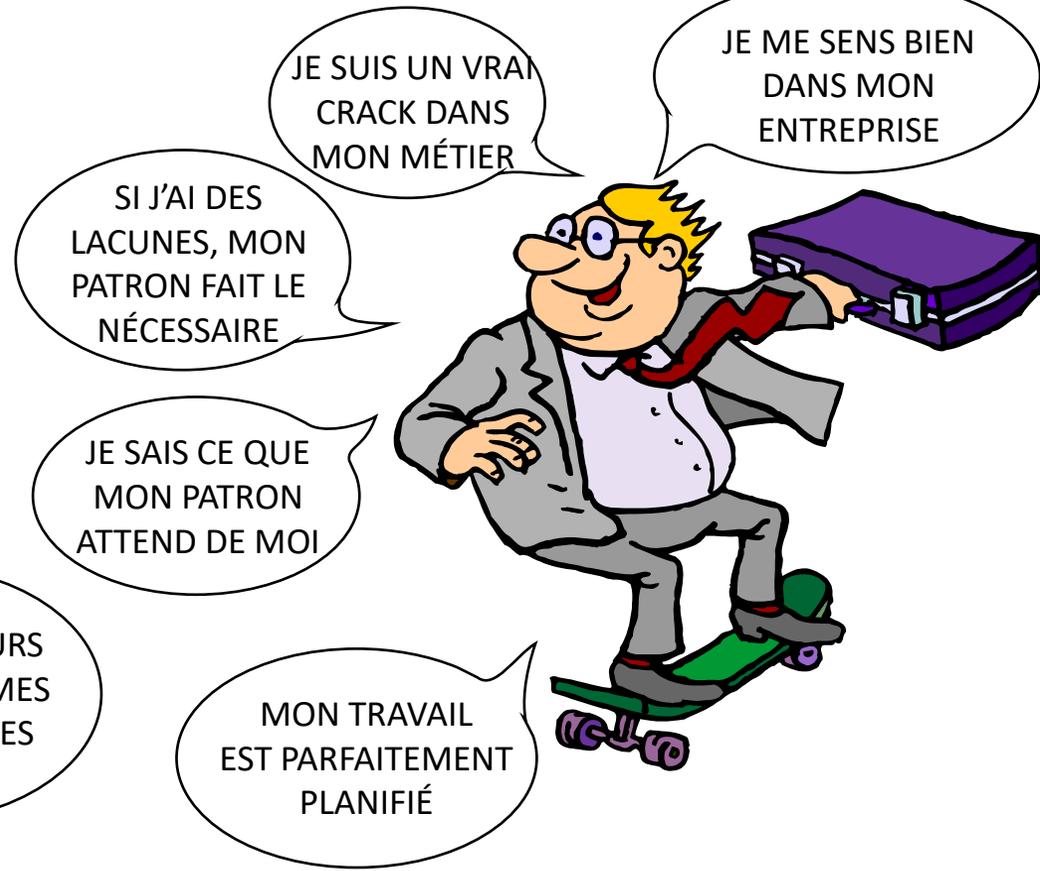
MON TRAVAIL EST PARFAITEMENT PLANIFIÉ

MES COLLABORATEURS CONNAISSENT MES OBJECTIFS ET LES RESULTATS

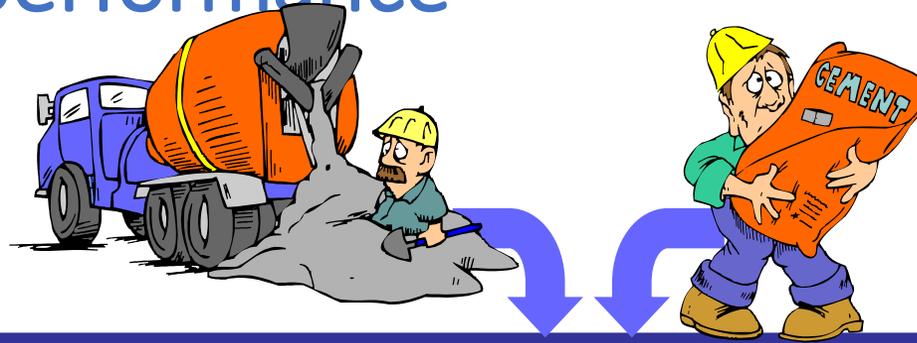
JE SUIS UN VRAI CRACK DANS MON MÉTIER

JE ME SENS BIEN DANS MON ENTREPRISE

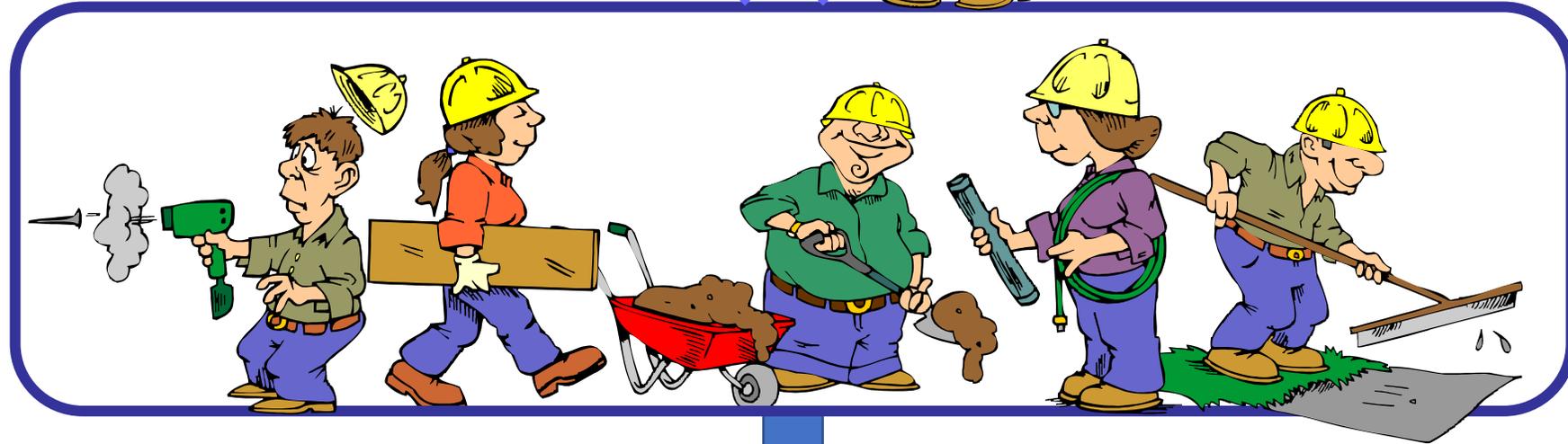
IMPLICATION DU PERSONNEL



Les 7 fondamentaux de la performance



**APPROCHE
PROCESSUS**



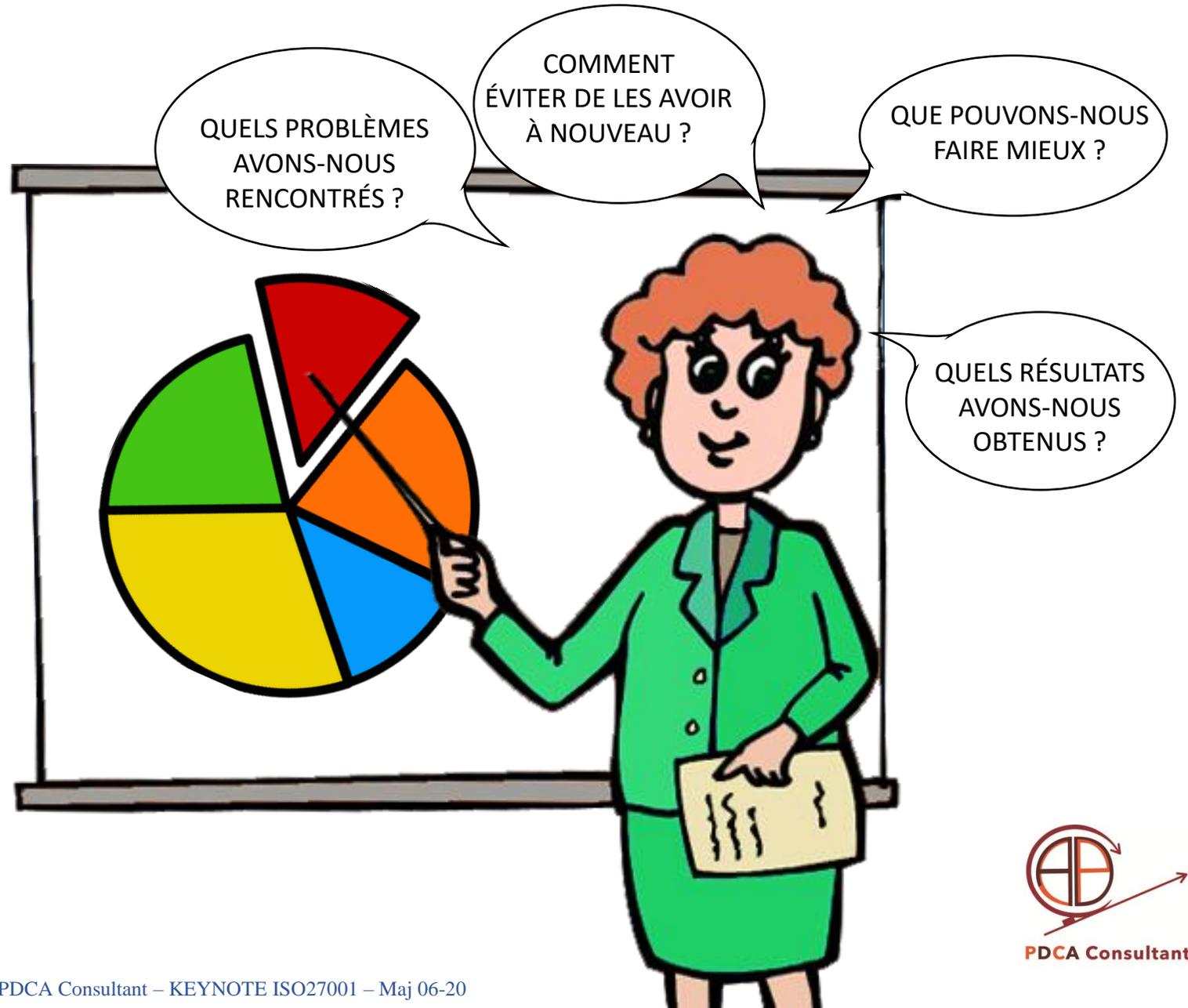
Les activités sont organisées
et permettent d'obtenir
le résultat attendu



PDCA Consultant

Les 7 fondamentaux de la performance

**AMÉLIORATION
ET PRISE DE
DÉCISION
FONDÉE SUR
DES PREUVES**



Les 7 fondamentaux de la performance

MANAGEMENT DES RELATIONS AVEC LES PARTIES INTÉRESSÉES



NOUS NOUS APPROVISIONNONS
AUPRES DE PRESTATAIRES CAPABLES
DE REPENDRE A NOS BESOINS

NOUS NOUS ASSURONS QUE LES
PRODUITS ET SERVICES QUE NOUS
LEUR DEMANDONS SOIENT
CONFORMES A NOS BESOINS

NOUS LEUR PASSONS
DES COMMANDES
CLAIRES ET PRECISES

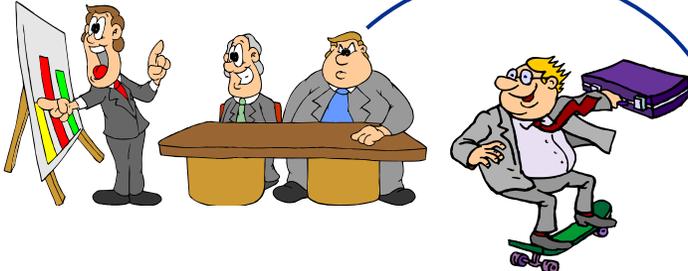
NOUS TRAVAILLONS
AVEC EUX EN BONNE
INTELLIGENCE

Les fournisseurs, les prestataires.. mais pas uniquement

Organisation de l'entreprise = pilotage du SMSI

JE SUIS TRÈS SATISFAIT

JE SAIS POURQUOI...



Synthèse de la démarche

ETAPE 4

- * Actions correctives
- * Actions préventives
- * Actions d'amélioration

ETAPE 3

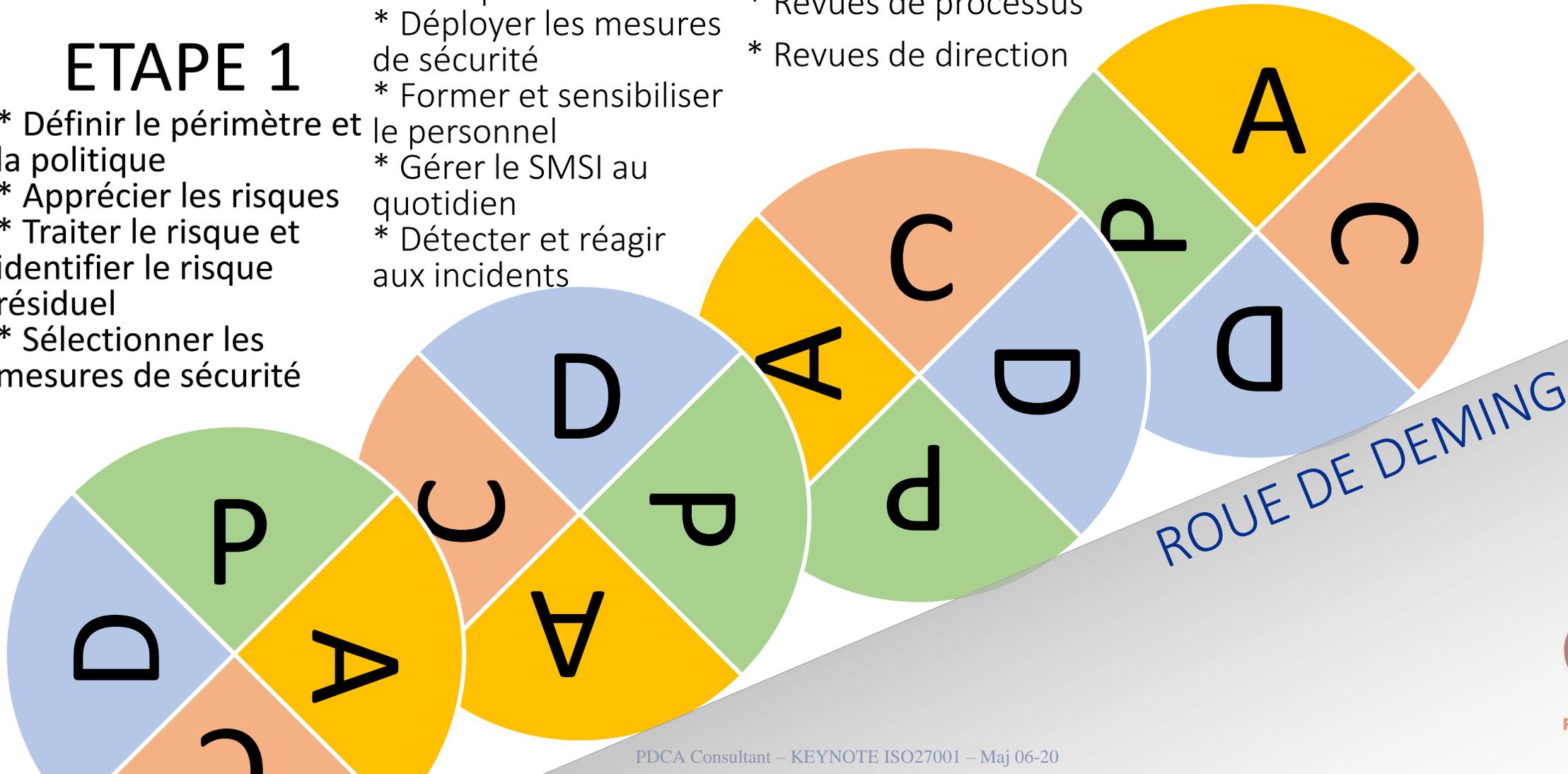
- * Audits internes
- * Contrôle interne
- * Revues de processus
- * Revues de direction

ETAPE 2

- * Plan de traitement des risques
- * Déployer les mesures de sécurité
- * Former et sensibiliser le personnel
- * Gérer le SMSI au quotidien
- * Détecter et réagir aux incidents

ETAPE 1

- * Définir le périmètre et la politique
- * Apprécier les risques
- * Traiter le risque et identifier le risque résiduel
- * Sélectionner les mesures de sécurité

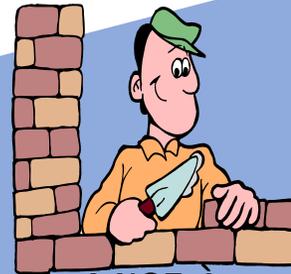
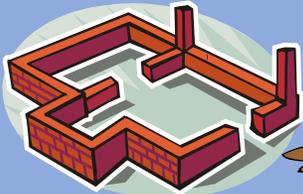


Du Diagnostic Initial à l'amélioration des performances... Puis CERTIFICATION

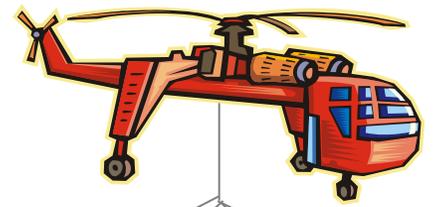
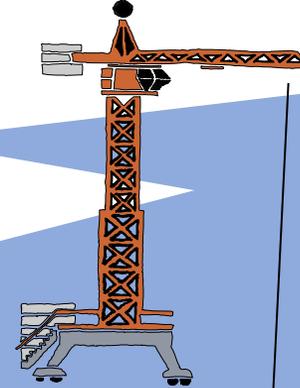
CAPITALISATION ET RETOUR
DE L'EXPÉRIENCE ET DES
BONNES PRATIQUES



SENSIBILISATION



MISE À
NIVEAU



AMÉLIORATION DES
PERFORMANCES



VALORISATION DE
LA DÉMARCHE

DIAGNOSTIC



AUDIT A BLANC



PDCA Consultant

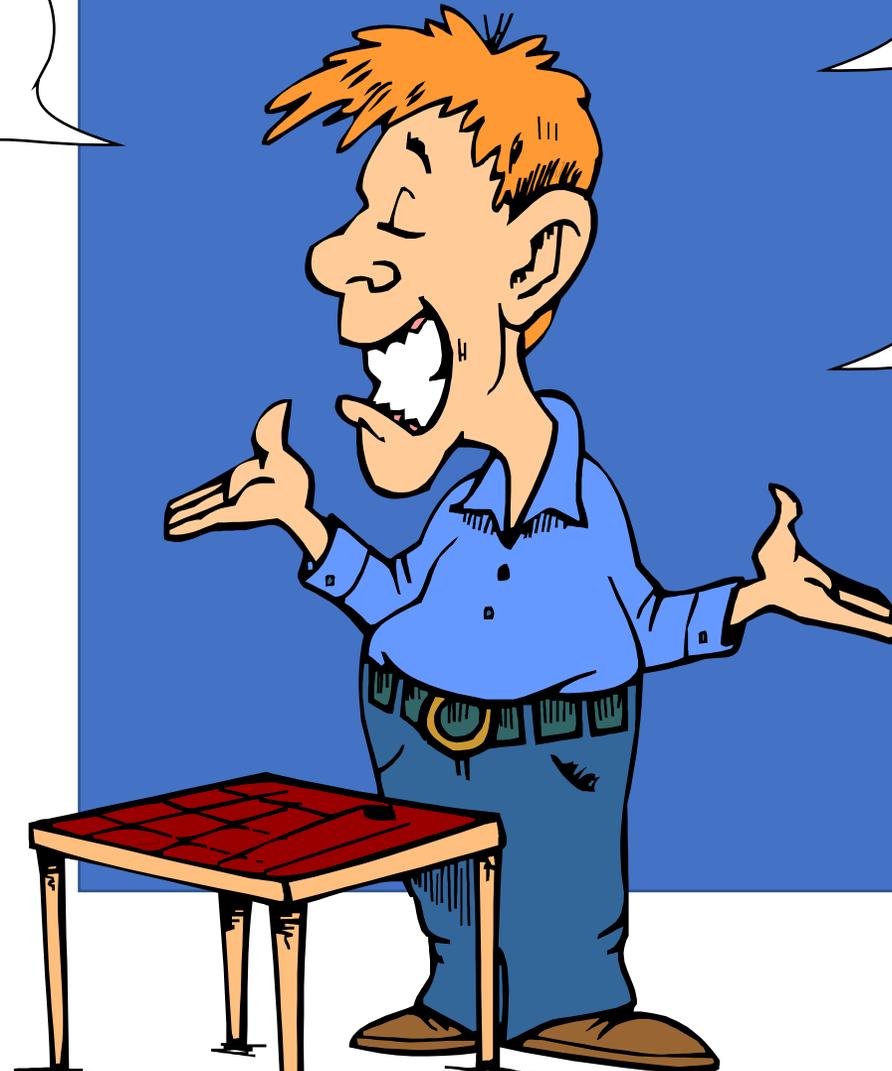
LA CERTIFICATION

Valable
3ans

Avec un audit
de suivi annuel

Délivrée par
un organisme
accrédité

ISO
27001



Principales difficultés Évoquées par le certifiés



Gestion charge
de travail (77%)

Disponibilité des
collaborateurs
(59%)

Gestion du
changement
(75%)

Compréhension
de la norme
(65%)

Qualification des
collaborateurs
(39%)

Disponibilité de
prestataires extérieurs
(17%)

Manque de soutien de la
direction (13%)

MERCI POUR VOTRE ECOUTE !



QUOI,
C'EST DÉJÀ FINI
?



AH BON,
DÉJÀ ?...

EN TOUT CAS,
MOI J'AI COMPRIS
CE QUE JE VAIS
FAIRE...



APRÈS TOUT,
CE N'EST QUE
DU BON SENS...



POUR ALLER PLUS LOIN

Inscrivez vous à la WEB-CONFERENCE AFNOR ISO27001

- Le 26/06 de 9h30 à 11h00

<https://www.afnor.org/evenement/web-conference-securite-information-bien-protege/>

OU CONTACTEZ-MOI



Max Ducros
07 76 88 46 50

Conseil / Formation / Audit
Ingénieur / Consultant / Formateur

Management de Projet,
de la qualité et des risques

contact@pdca-consultant.fr

