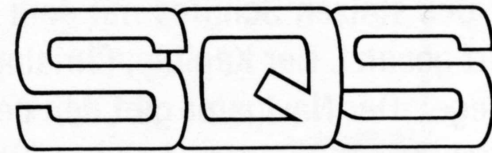


Cordiale bienvenue
à la conférence



**Sécurité, qualité,
management
démarches ISO 27001, 9001,
20000
Système de Management ?
Intégré ?**

Sécurité, qualité, management démarches ISO 27001, 9001, 20000

Sommaire



- 0. Présentation de la SQS**
- 1. Contexte**
- 2. ISO/IEC 27001:2005**
- 3. ISO 9001:2000**
- 4. ISO/IEC 20000**
- 5. Vers un Système de Management Intégré**
- 6. Conclusions**

Sécurité, qualité, management

0. Présentation de la SQS

- Association Suisse pour
Systèmes
- de Qualité et de
Management

- Bernstrasse 103, CH-3052 Zollikofen
- +41 31 910 35 35
- headoffice@sqs.ch
- www.sqs.ch



Sécurité, qualité, management

1. Contexte: questions ouvertes fréquemment rencontrées

- La quête vers le Saint Graal de la sécurité informatique, atteindre un niveau optimal, est elle longue et difficile ?
- La norme ISO 2700x est elle le Saint Calice de cette quête ?
- La démarche ISO 2700x est-elle comparable à une politique de qualité au sens industriel du terme ?
- Simple guide de bonnes pratiques ou démarche de progrès ?
- Quels sont les liens avec le management du risque ?
- Permet-elle d'assurer une certaine forme de pérennité quant au niveau de sécurité ?
- Liens avec ISO9001, avec ISO 20000 (management du SI)



Sécurité, qualité, management

1. Contexte: questions ouvertes fréquemment rencontrées

- Quel intérêt pour les petites structures : mairies, PME/PMI, start-up, services administratifs, universités, centres de recherche ?
- ...
- ...
- ...
- et d'autres encore ?
- ...
- ...
- Réponses potentielles et pistes de réflexions ?



Sécurité, qualité, management

2. ISO/IEC 27001:2005



ISMS

Information Security Management System

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005

• Version 3.02, March 2007



Sécurité, qualité, management

2. ISO/IEC 27001:2005: nombre de références

Japan	2354*	Spain	12	Sri Lanka	3
India	387	Switzerland	12	Vietnam	3
UK	374	UAE	12	Belgium	2
Taiwan	165	Saudi Arabia	10	Bulgaria	2
China	101	France	8	Denmark	2
Germany	93	Iceland	8	Lithuania	2
Hungary	60	Sweden	8	Oman	2
Korea	59	Greece	7	Peru	2
USA	59	Pakistan	7	Portugal	2
Australia	53	Kuwait	6	Qatar	2
Italy	45	Russian Federation	6	Armenia	1
Netherlands	32	Slovenia	6	Egypt	1
Hong Kong	30	Thailand	6	Gibraltar	1
Czech Republic	28	Slovakia	5	Lebanon	1
Singapore	28	Argentina	4	Luxemburg	1
Malaysia	22	Bahrain	4	Macedonia	1
Austria	21	Canada	4	Moldova	1
Poland	21	Romania	4	Morocco	1
Brazil	18	Chile	3	New Zealand	1
Ireland	18	Colombia	3	Ukraine	1
Finland	14	Croatia	3	Uruguay	1
Norway	14	Indonesia	3	Yugoslavia	1
Turkey	14	Isle of Man	3		
Mexico	12	Macau	3	Relative Total	4229
Philippines	12	South Africa	3	Absolute Total	4209*



Sécurité, qualité, management

2. ISO/IEC 27001:2005: références en France



Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Axalto SA, Tours PSC	France	LSTI/SMSI/01	LSTI SAS RCS	BS 7799-2:2002
CMA France S.A.R.L.	France	IS 97256	BSI	BS 7799-2:2002
EADS Security Networks	France	07 05 00 00	Bureau Veritas Certification	ISO/IEC 27001:2005
EMAILING SOLUTION	France	159 79 26	Bureau Veritas Certification	ISO/IEC 27001:2005
IBM ITD France	France	06039905	Bureau Veritas Certification	ISO/IEC 27001:2005
KDDI France	France	07 02 00 00	Bureau Veritas Certification	ISO/IEC 27001:2005
ODISO and Emailing Solutions	France	159 79 26/A	Bureau Veritas Certification	ISO/IEC 27001:2005
Verio Europe	France	LRQ4001385	LRQA	ISO/IEC 27001:2005

Référence: <http://www.iso27001certificates.com/>

Sécurité, qualité, management

2. ISO/IEC 27001:2005: références en Suisse



Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
ACM Advanced Currency Markets SA	Switzerland	GB07/72810	SGS United Kingdom Limited	ISO/IEC 27001:2005
AlpTransit Gotthard AG	Switzerland	13827	SQS	BS 7799-2:2002
Beda Informatik AG	Switzerland	30671	SQS	BS 7799-2:2002
innova Versicherungen AG, innova Krankenversicherung AG	Switzerland	30768	SQS	BS 7799-2:2002
Reuters SA	Switzerland	IS 509254	BSI	ISO/IEC 27001:2005
RTC Real Time Center AG, Liebefeld	Switzerland	20279	SQS	BS 7799-2:2002
Serono International S.A.	Switzerland	GB05/64392	SGS United Kingdom Limited	BS 7799-2:2002
Serono International SA The Information Technology Function	Switzerland	GB05/64392	SGS United Kingdom Limited	ISO/IEC 27001:2005
SRG SSR idée suisse	Switzerland	20794	SQS	BS 7799-2:2002
Swiss Post Post Finance Information Technology, Berne	Switzerland	001 / 2002	KPMG SA	BS 7799-2:2002
Swisscom IT Services AG	Switzerland	11992	SQS	BS 7799-2:2002
T-Systems Schweiz AG, Switzerland	Switzerland	304444 IS	DQS GMBH	BS 7799-2:2002

Référence: <http://www.iso27001certificates.com/>

Sécurité, qualité, management

3. ISO 9001:2000



La série des normes ISO 9000:2000



Sécurité, qualité, management

4. ISO/IEC 20000

Systemes de management
pour les prestations de services
informatiques.

Meilleures pratiques pour la mise en œuvre.

- ISO/IEC 20000-1:2005
- ISO/IEC 20000-2:2005

Version 3.02, March 2007



Sécurité, qualité, management

5. Vers un Système de Management Intégré



- Le périmètre d'un système de management **intégré** se voit élargi à:
 - d'autres normes et/ou à de parties intéressées ou prenantes
 - à d'autres besoins contextuels que ceux du client
- « L'adoption d'un Système de Management **Intégré** relève d'une décision **stratégique** de l'organisme.
- Sa conception et sa mise en œuvre **tiennent compte des besoins contextuels**, afin d'identifier les processus **nécessaires** au **SMI** ainsi que leur application dans le périmètre spécifié de l'organisme.

Sécurité, qualité, management

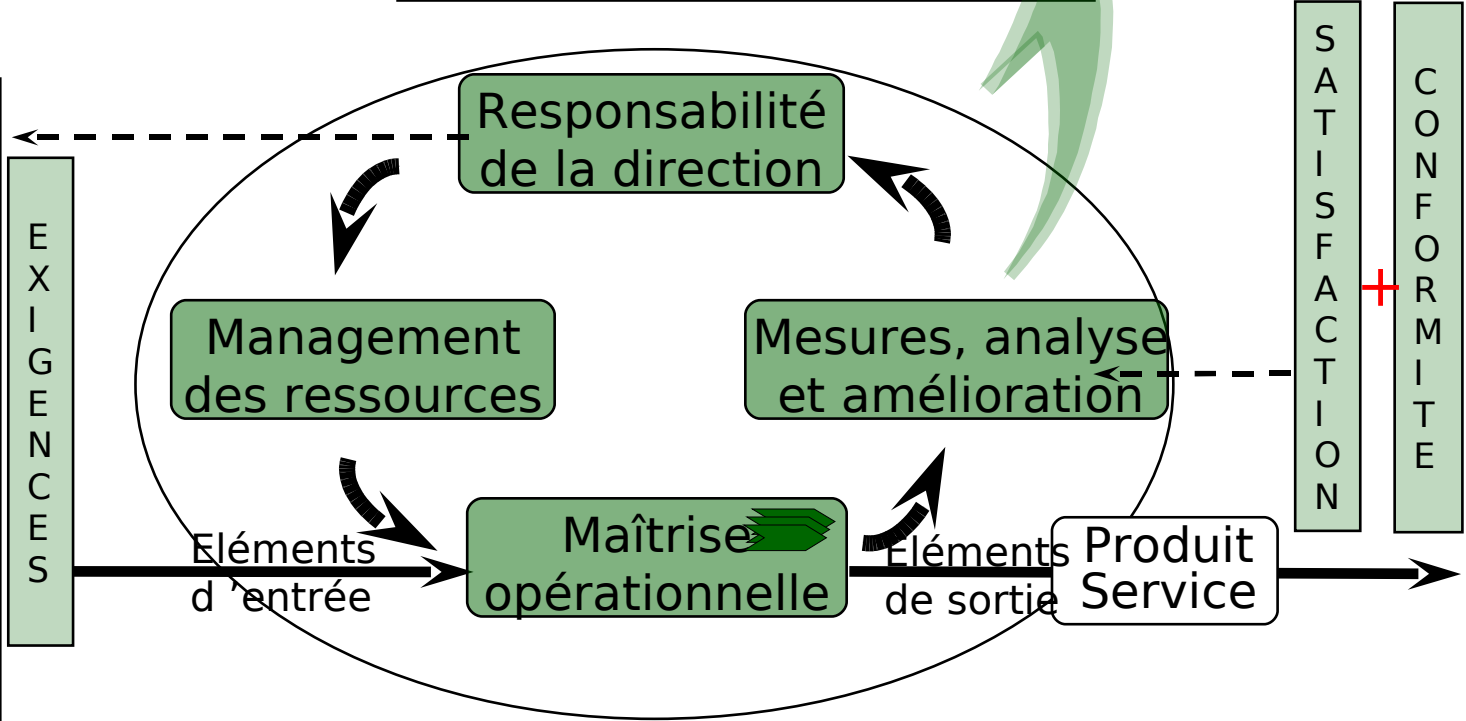
5. Vers un Système de Management Intégré

- Orientations des normes
- Conformité réglementaire et légales
 - Engagement à la prévention
 - Amélioration continue des performances d'exploitation de service, produits métier, sécurité, ..., et du système de management



Amélioration continue du système de management

- «Client S»
- Clients
 - Actionnariat
 - Autorités
 - Personnel
 - Société
 - L'entreprise
 - Groupe
 - ...



- «Client S»
- Clients
 - Actionnariat
 - Autorités
 - Personnel
 - Société
 - L'entreprise
 - Groupe
 - ...

Sécurité, qualité, management

6. Conclusions

Quelle norme dans quel contexte ?

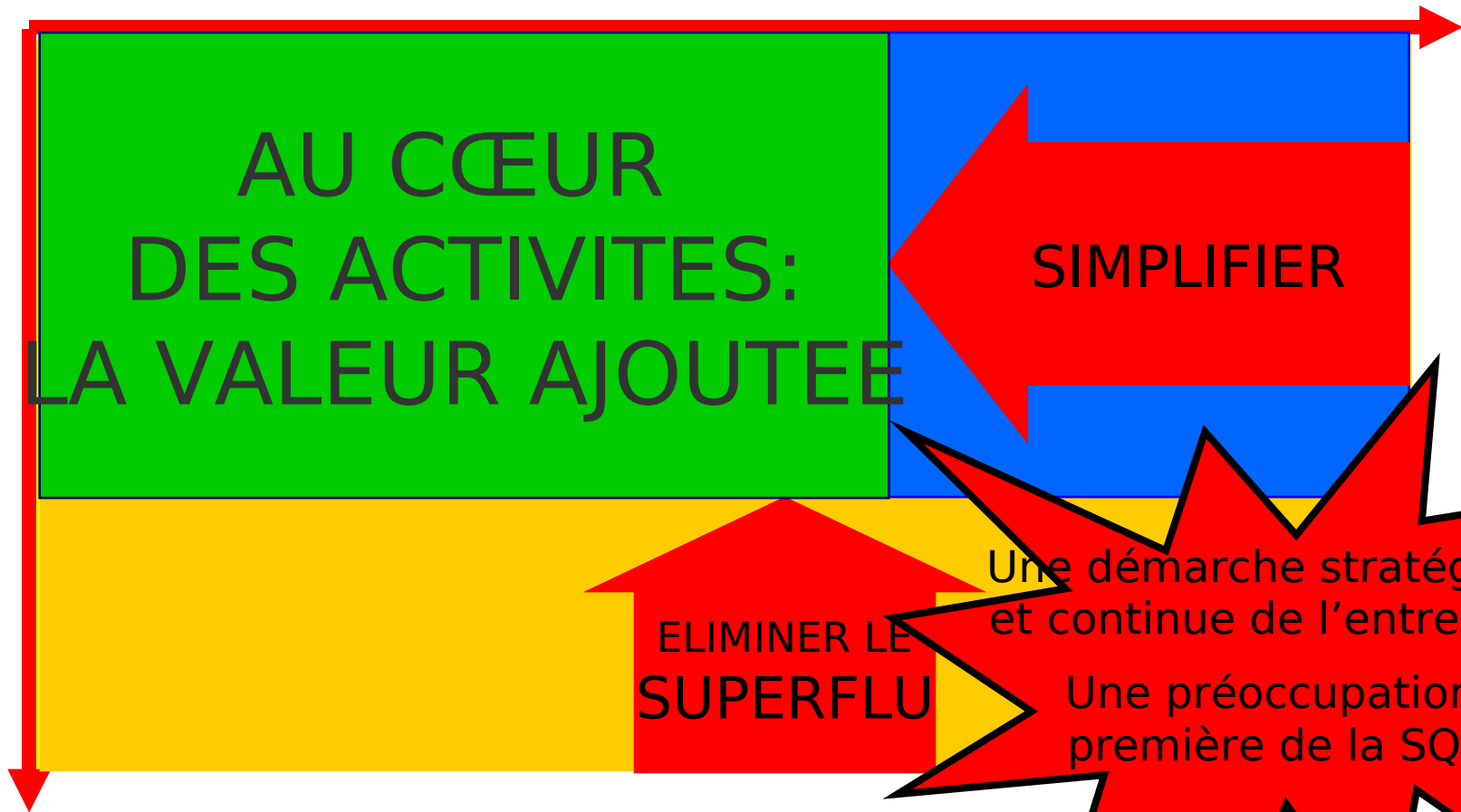


- Système de management lorsque les besoins de sécurité internes et/ou externes sont un pré-requis pour assurer la qualité de service
- Système de management, dans le sens large du terme
- Système de management consacrée spécifiquement à la gestion des services informatiques (production métier)

Sécurité, qualité, management

COMPLEXITE DES ACTIVITES

VOLUME / Nbre D'ACTIVITES



SQS

Discussion



S

Association Suisse pour Systèmes de Qualité et de Management

Adresse du siège de la SQS et secrétariat francophone			
SQS Bernstrasse 103 CH - 3052 Zollikofen www.sqs.ch (en 4 langues)	Téléphone (français)	+41 (0)31 910 35 57	Carmen Hodel carmen.hodel@sqs.ch
		+41 (0)31 910 35 55	
	Téléphone central	+41 (0)31 910 35 49	
	Télécopie		



Contact en de l'intervenant				
Prénom et nom	Téléphone	Portable	Télécopie	Messagerie
Claude Otz	+41 (0)32 730 3088	+41 (0)79 406 1515	+41 (0)86 079 406 1515	claudio.otz@sqs.ch

La série des normes ISO 9000:2000

La série des normes ISO 9000:2000

ISO 9000:2000

**Systemes de management de la
qualité**

**Principes essentiels et
vocabulaire**

ISO 9001:2000

**Systemes de management de la
qualité**

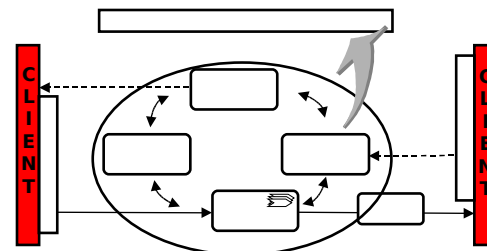
Exigences

ISO 9004:2000

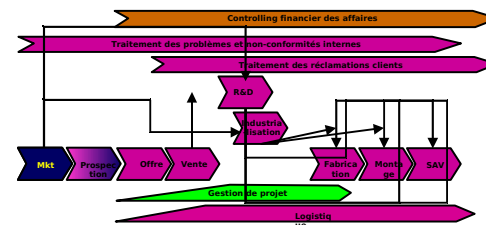
**Systemes de management de la qualité
Lignes directrices pour l'amélioration des
performances**

ISO 9000:2000 - Ses axes forts

儻 **Orientation client**



儻 **Méthode axée sur les processus/gestion des processus**



儻 **Amélioration continue des processus et du système de management**



ISO 9000:2000 - Les huit principes du Management

1. **Organisme à l'écoute du client:**

Comprendre et réaliser leurs besoins présents et futurs

2. **Leadership:**

Définir une politique interne de l'organisme. Mettre en mouvement les collaborateurs afin de les faire contribuer à la concrétisation de la stratégie et des objectifs de l'organisme

3. **Personnel:**

L'implication de tous les collaborateurs permet d'utiliser leurs capacités au profit de l'organisme

4. **Approche processus:**

Gérer les moyens et activités qui lui sont liés comme un processus

5. **Management par approche système:**

Comprendre et gérer un système de processus interdépendants

6. **Amélioration continue:**

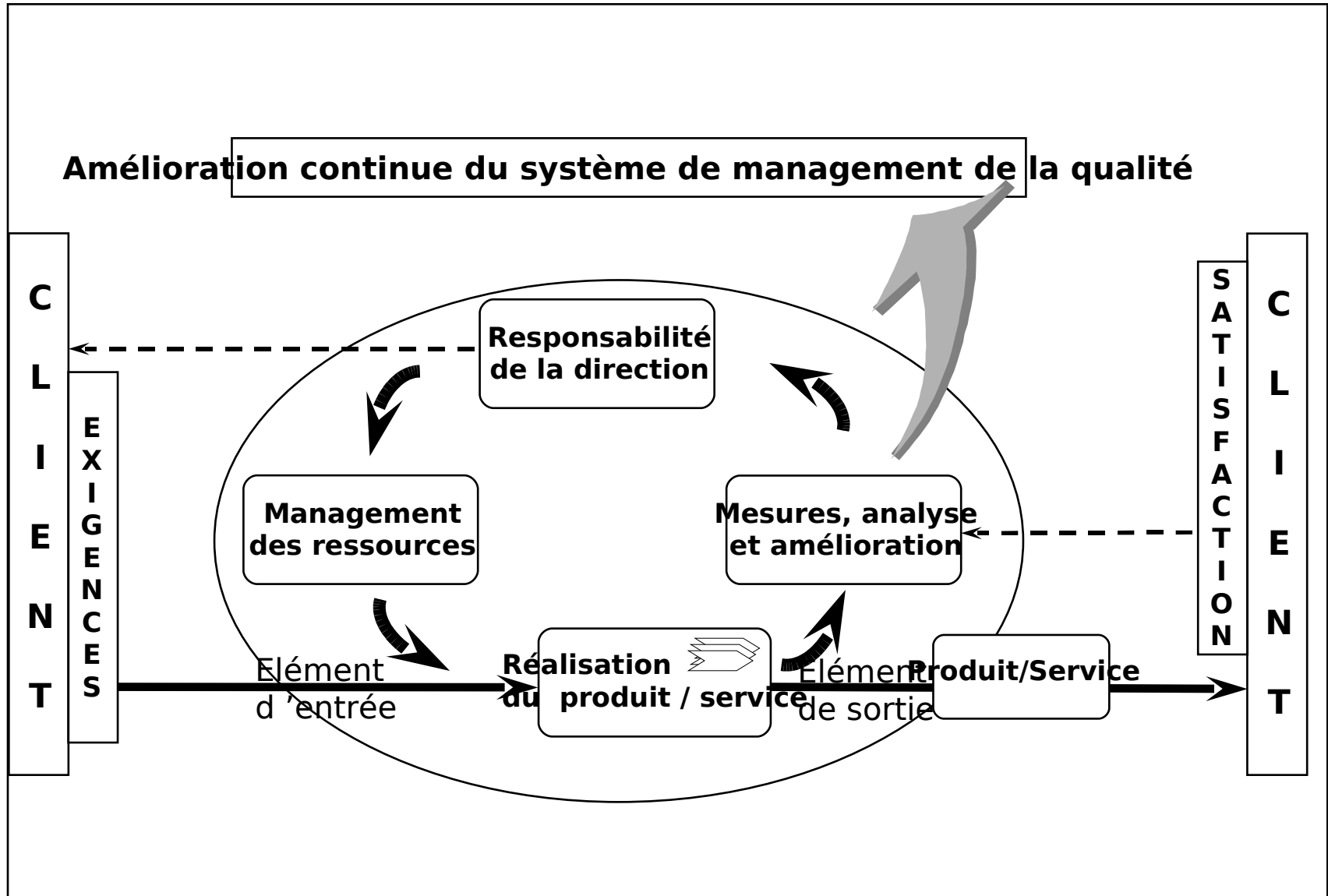
Objectif permanent de l'organisme

7. **Approche factuelle pour la prise de décision:**

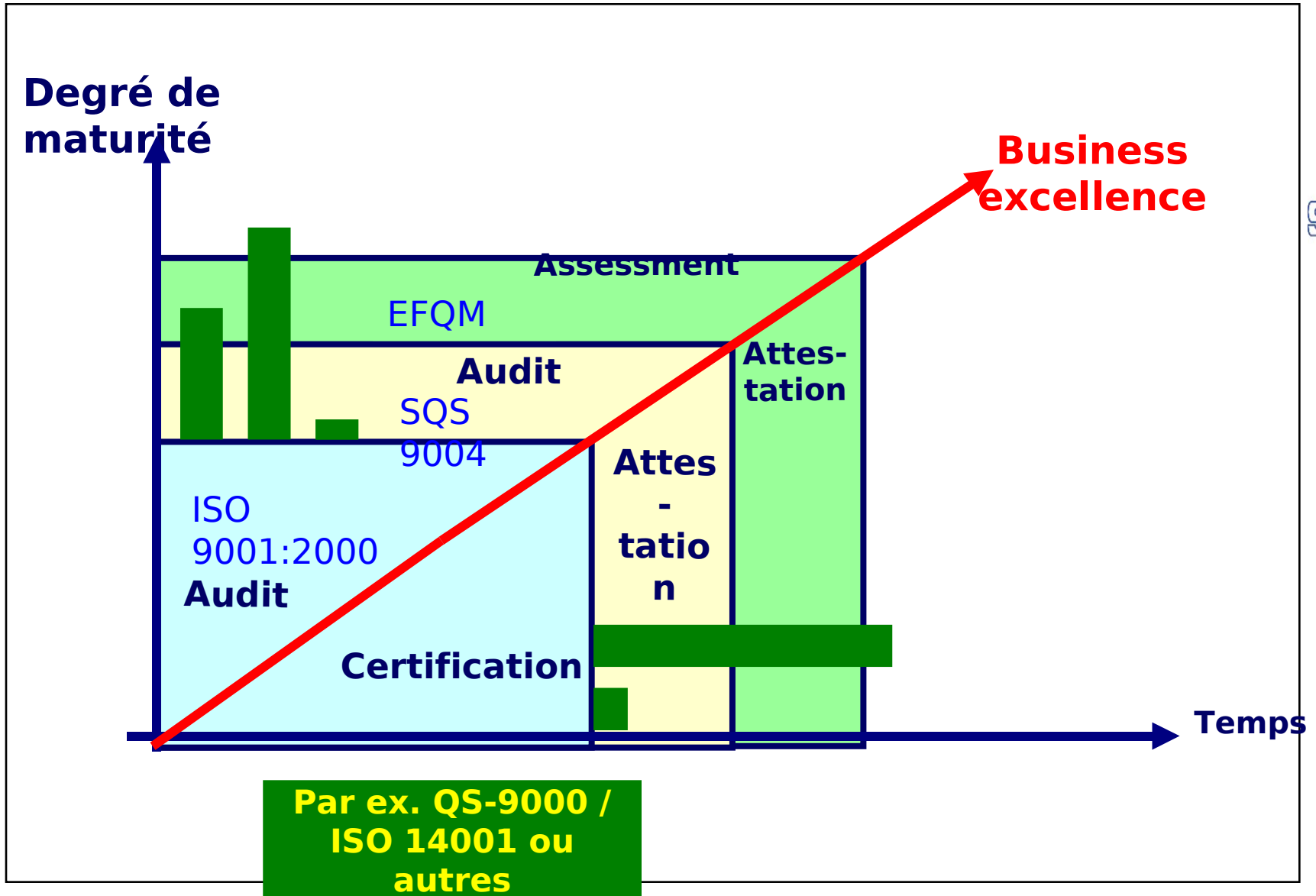
Sur la base d'une analyse logique et intuitive

8. **Relations mutuellement bénéfiques avec les fournisseurs**

ISO 9000:2000 - Son modèle



Base de l'évolution du SMQ d'une organisation



Généralités

- 儻 L'adoption d'un système de management est une **décision stratégique** pour la direction d'un organisme
- 儻 Aptitude de l'organisme à **garantir en permanence la conformité** de ses produits/prestations de service
- 儻 La mise en oeuvre **englobe toutes les activités** depuis les exigences de la clientèle jusqu'à sa satisfaction
- 儻 Possibilité de mise en oeuvre pour **tous les types d'organismes**, quelle que soit leur taille
- 儻 **Tous les processus déterminants** qui contribuent à la garantie de la conformité des produits/prestations de service doivent être inclus
- 儻 **Exclusion autorisée seulement pour processus de réalisation**, à justifier et à documenter (par ex.: conception et développement)

Exigences générales

- 儻 **Identification et gestion des processus** de l'organisme (architecture des processus)
- 儻 Détermination de la **séquence** et de **l'interaction** des processus
- 儻 **Critères et méthodes** nécessaires à la **gestion des processus** (mesures des résultats des processus et de leur efficacité, amélioration continue)
- 儻 **Garantie** de la disponibilité des **ressources** et informations nécessaires au fonctionnement et à la gestion des processus
- 儻 **Amélioration continue** des processus et du système de management

Exigences générales relatives à la documentation

- ☞ Adaptation de la **documentation en fonction des besoins** (genre d'organisme, complexité, qualification et compétences)
- ☞ Garantie de l'**efficacité de la planification**, de la réalisation et de la gestion des processus
- ☞ Manuel sur le système de management (instrument de conduite axé sur les besoins internes)
- ☞ Bases de la maîtrise des documents
- ☞ Enregistrements relatifs à la qualité, principes, sécurité des preuves

Responsabilité de la direction (1/2)

☐ **Engagement** de la direction (commitment) au développement et à l'amélioration du système de management (domaine d'application, totalité des processus)

☐ **Orientation client**

☐ **Evaluation des attentes et des exigences des clients, de même que des exigences légales**

☐ Mise en œuvre interne des attentes et exigences des clients

☐ Obtention de la **satisfaction des clients**

☐ **Politique de l'organisme**, politique qualité incluse

☐ **Processus relatif à la planification et à la définition** des objectifs

☐ Spécification des responsabilités et des compétences

Responsabilité de la direction (2/2)

☐ Représentant de la direction (membre de l'encadrement)

☐ **Communication interne**

☐ Éléments d'entrée de la revue de direction (clients, audits, gestion des processus)

☐ Données de sortie de la revue de direction (amélioration du système, amélioration des processus, amélioration du produit/de la prestation de service, besoins en ressources)

Management des ressources

儻 Management des ressources en adéquation avec les processus, conformité aux exigences de la clientèle pour parvenir à la satisfaction des clients

儻 Affectation du personnel, compétences et aptitudes

儻 Constat des compétences nécessaires (profils d'exigences)

儻 **Recrutement**, formation, qualification, maintien, **efficacité de la formation**, documentation

儻 **Infrastructure** (bâtiments, équipements, matériels, logiciels, services support)

儻 Maintenance

儻 Environnement professionnel pour la réalisation de produits/prestations de service conformes

Réalisation du produit/de la prestation de service (1/3)

盞 **Planification**, établissement et gestion des processus de réalisation

盞 Evaluation des exigences des clients (y compris directives, lois, service après-vente)

盞 Faisabilité

盞 **Communication avec les clients**

盞 Planification et maîtrise de la conception et du développement
(y compris évolution des processus au besoin)

盞 Données relatives à la conception et au développement (éléments d'entrée)

盞 Résultats de la conception et du développement (données de sortie)

盞 Revue de conception et de développement, vérification, validation,
documentation (adéquate, appropriée)

盞 Modifications de la conception et du développement

Réalisation du produit/de la prestation de service (2/3)

燈 Processus relatif aux achats

燈 Evaluation et sélection des fournisseurs

燈 Informations relatives aux achats

燈 Contrôle des produits/prestations de service achetés

燈 Maîtrise de la réalisation des produits/prestations de service
(toute la chaîne de valeur ajoutée, service après-vente inclus)

燈 Maîtrise des processus de réalisation (y compris **validation** des processus,
et le cas échéant application de la systématique de conception)

燈 **Validation** des processus pour lesquels le résultat peut seulement
être constaté après la livraison

Réalisation du produit/de la prestation de service (3/3)

儻 Identification, traçabilité

儻 **Propriété du client**

儻 Préservation des produits/prestations de service (pendant la réalisation et jusqu'à la livraison incluse)

儻 Maîtrise des dispositifs de mesure et de surveillance

儻 **Méthodes de mesure adéquates pour assurer la conformité et réaliser des améliorations**



儻 Mesure de la **satisfaction du client** et perception de la prestation réalisée

儻 Audits internes (conformité et efficacité du système de management)

儻 **Mesures et améliorations des processus** en vue d'obtenir les résultats planifiés

儻 Mesures des produits/prestations de service dans le but de satisfaire aux exigences (exigences des clients, exigences légales, etc.)

Mesures, analyses et amélioration (2/2)

罫 Traitement des produits/prestations de service non-conformes

罫 Collecte et analyse des données pour l'amélioration du système de management (satisfaction du client, conformité des produits/prestations de service, caractéristiques des processus et trends, fournisseurs)

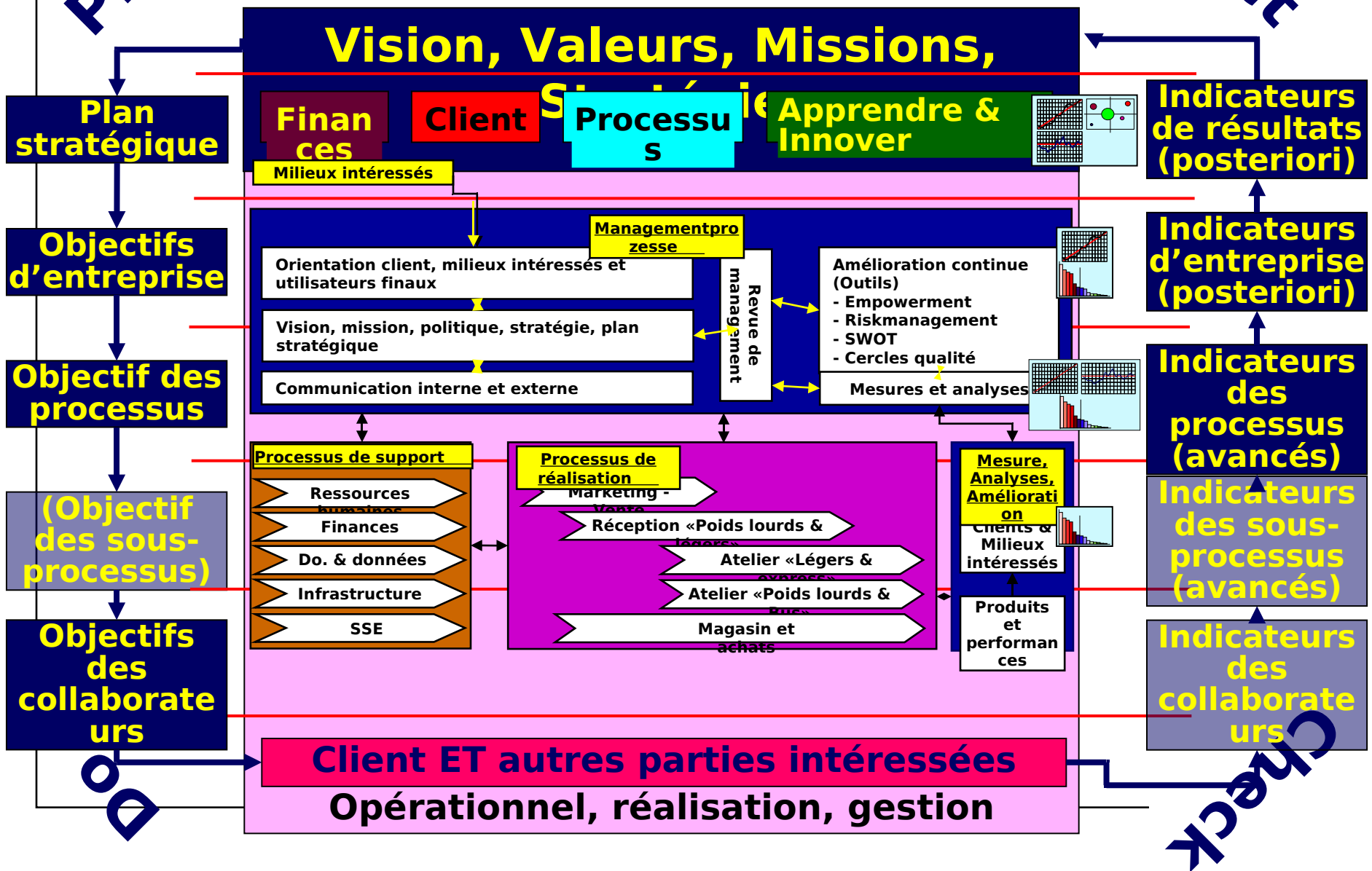
罫 **Processus d'amélioration continue** des processus et du système de management

罫 Actions correctives, analyse des causes et actions pour empêcher que les non-conformités ne se reproduisent

罫 Actions préventives, identification et élimination des causes de non-conformités potentielles

**En conclusion, la vision
SQS de la série des
normes ISO 9000:2000**

Plan ISO 9000:2000 - Sa philosophie



Systemes de management pour les prestations de services informatiques. Meilleures pratiques pour la mise en œuvre.

- ISO/IEC 20000-1:2005
- ISO/IEC 20000-2:2005

Les bases

- Les meilleures pratiques de l'**IT Infrastructure Library (ITIL)** ont été développées par l'Office of Government Commerce (OGC) à Norwich, Angleterre, sur mandat du Gouvernement britannique.
- L'ITIL décrit l'objectif à atteindre.
- La manière de l'atteindre est laissée à aux soins des entreprises.
- **L'ISO 9001** est une norme décrivant les exigences posées à un système de management, indépendamment du secteur d'activité considéré.
- **ISO 9001** ⇒ **certification d'organisations**
- L'IT Service Management Forum (**itSMF**) est l'association des utilisateurs de l'ITIL.
- **ISO/IEC 20000** ⇒ **certification de prestations informatiques commerciales**
- **ISO/IEC 20000** ⇒ **est entrée en vigueur le 15.12.2005 et remplace la BS 15000**
- **Les certificats BS 15000 devaient être adaptés à l'ISO/IEC 20000 pour le milieu de l'année 2007**

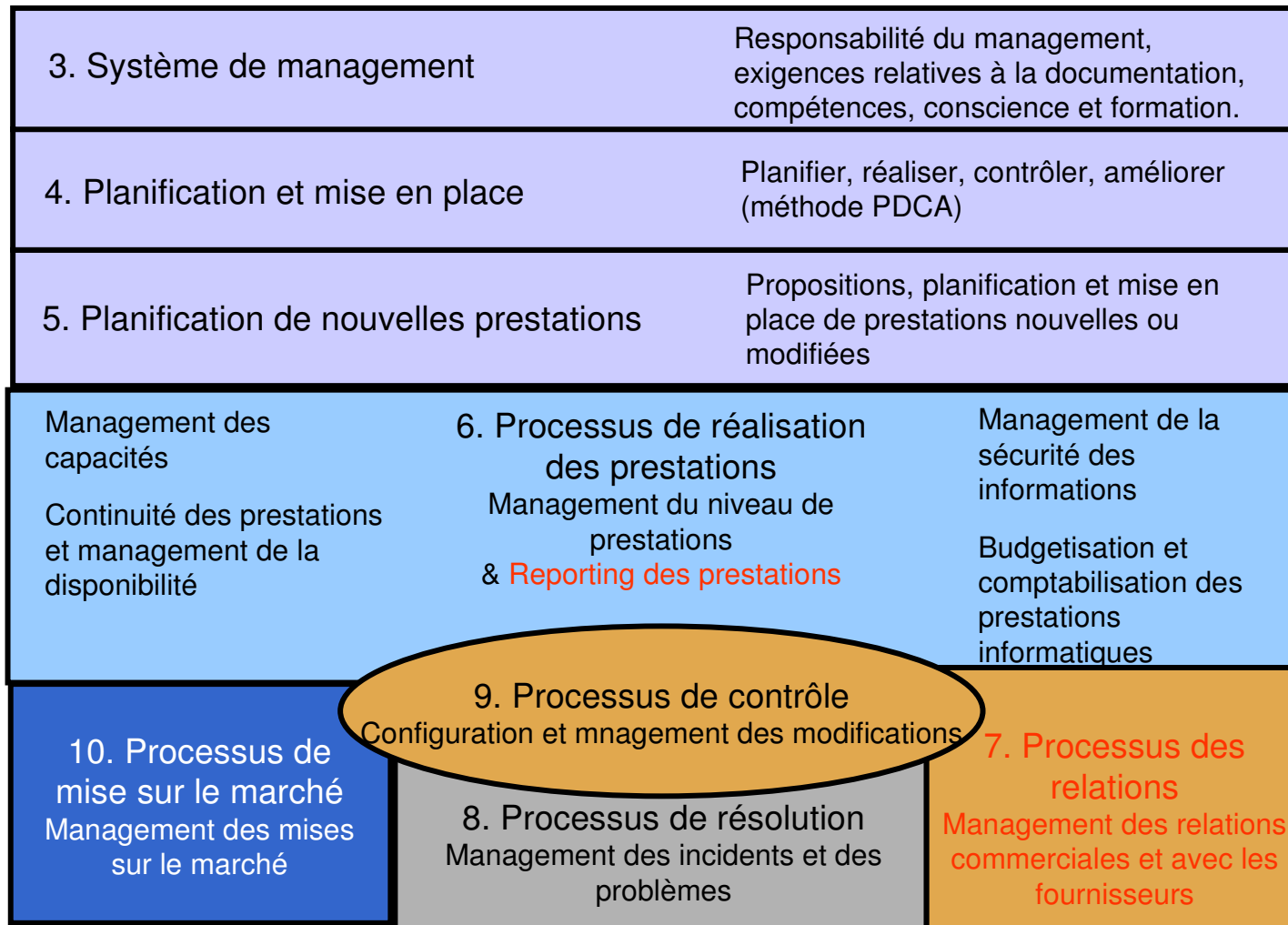
Avantages de l'ISO/IEC 20000

- Meilleure communication entre les secteurs informatique et commercial, sur la base de descriptions des prestations et de chiffres clé définis dans des SLA
- Des bases contractuelles claires pour l'ensemble de la chaîne de fournisseurs réduisent les risques liés aux prestations commerciales
- Amélioration permanente du management des prestations sur la base de chiffres clé relatifs à la qualité
- Réduction des coûts à long terme pour le développement et la fourniture de prestations
- Productivité accrue et meilleure mise à profit des compétences et de l'expérience

Structure de l'ISO/IEC 20000-1

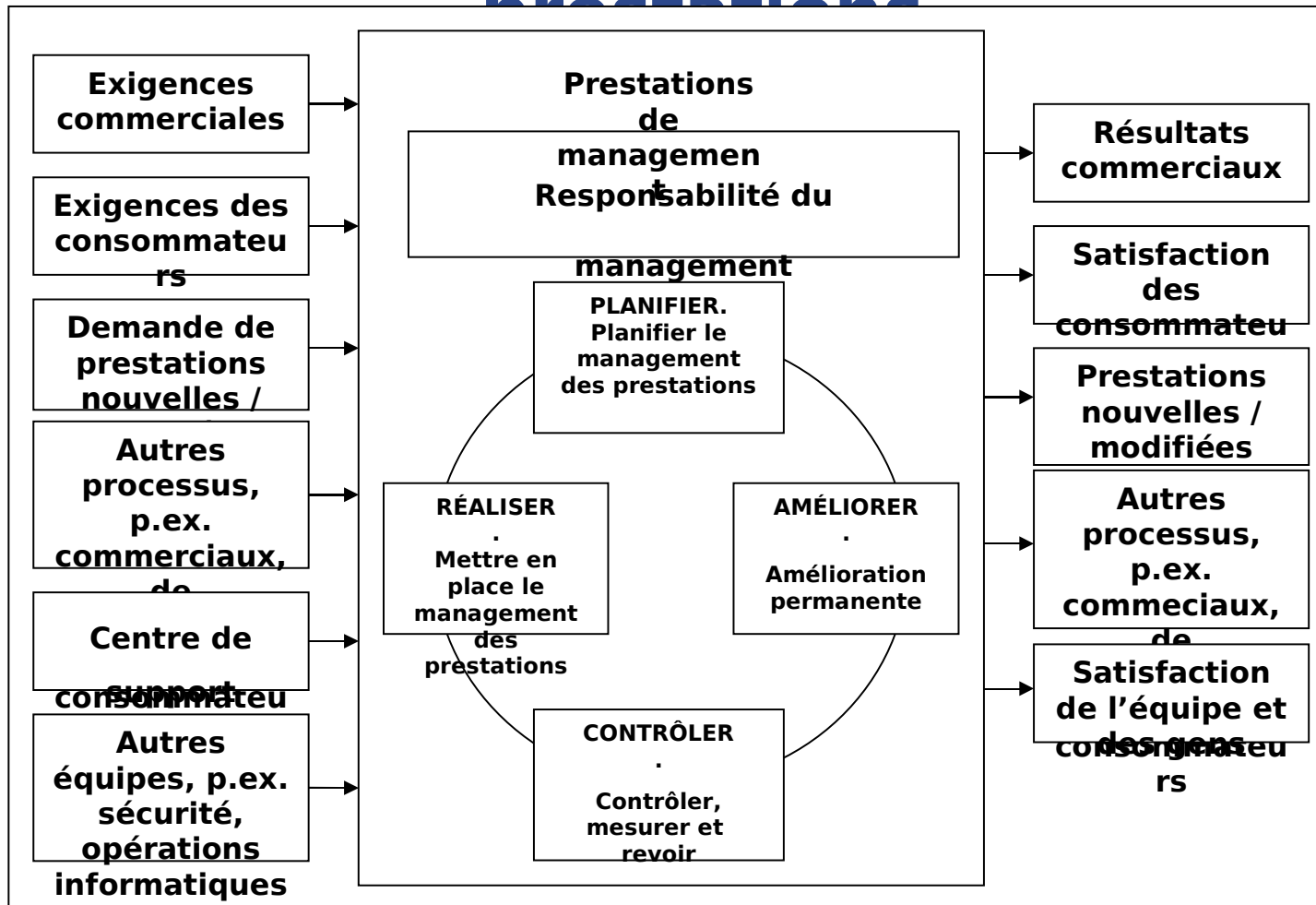
1. Objectif

2. Terminologie et définitions



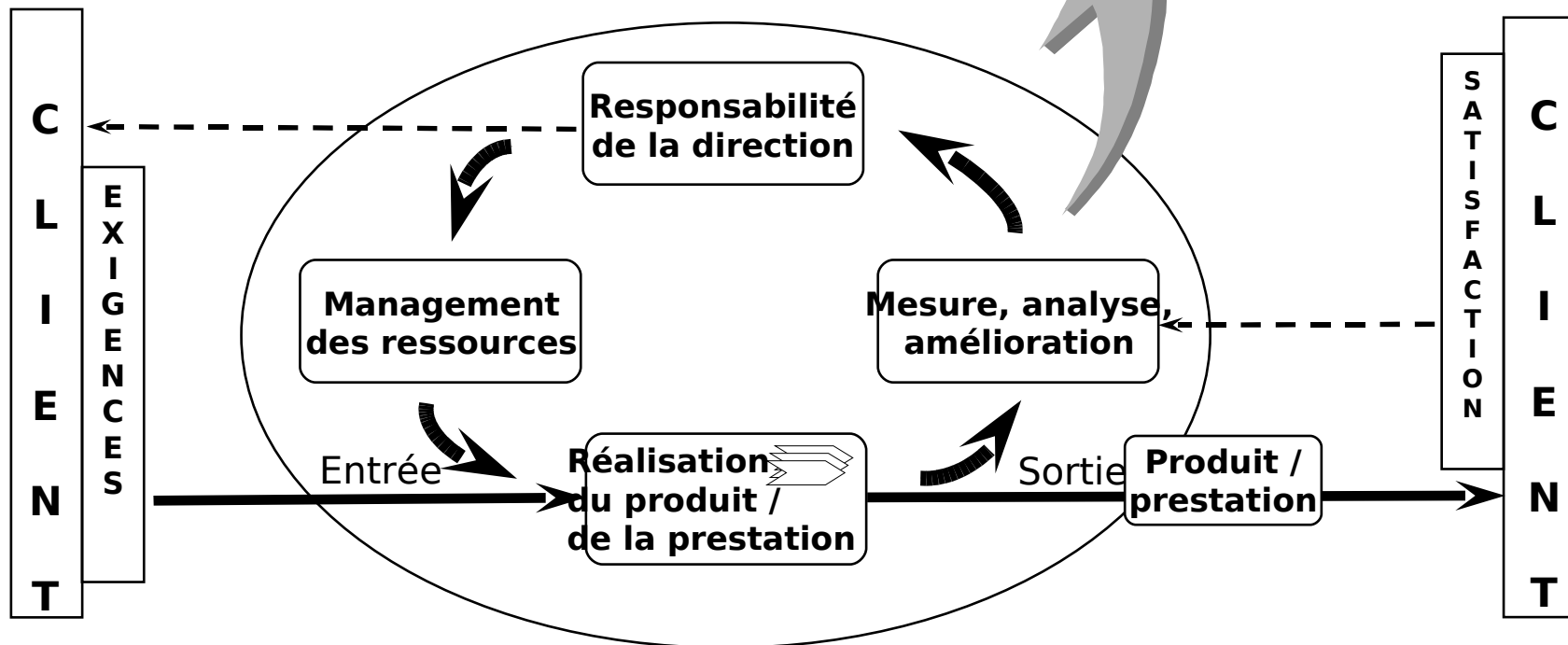
Méthode PDCA

(planifier - réaliser - contrôler - améliorer)
pour les processus du management des prestations



Modèle de système de management de la qualité orienté processus (ISO 9001:2000)

Amélioration permanente du système de management de la qualité



ITIL V3 - cycle de vie des prestations la structure centrale



Contenu de l'ISO/IEC20000-1 (1)

3. Exigences posées à un système de management des prestations (SMP)

- Engagement du management
- Exigences liées à la documentation
- Compétences, conscience, formation et perfectionnement

Contenu de l'ISO/IE 20000-1 (2)

- **Planification et réalisation du management des prestations**
 - Planification du management des prestations (planifier)
 - Mise en œuvre du management des prestations et réalisation des prestations (réaliser)
 - Surveillance, mesure et contrôle (contrôler)
 - Amélioration permanente (améliorer)

Contenu de l'ISO/IEC 20000-1 (3)

5. Planification et mise en place de prestations nouvelles ou modifiées

- Réalisation de l'offre
- Planification sur la base d'un management formel des modifications
- Mise en place ou modification des prestations
- Rapport des prestataires de services
- Rapport final (revue après mise en place)

Contenu de l'ISO/IEC 20000-1 (4)

- **Processus de réalisation des prestations**
 - Service Level Management (SLA)
 - Reporting des prestations
 - Disponibilité et management de la continuité des prestations
 - Budgétisation et comptabilisation des prestations informatiques
 - Management des capacités
 - Management de la sécurité des informations

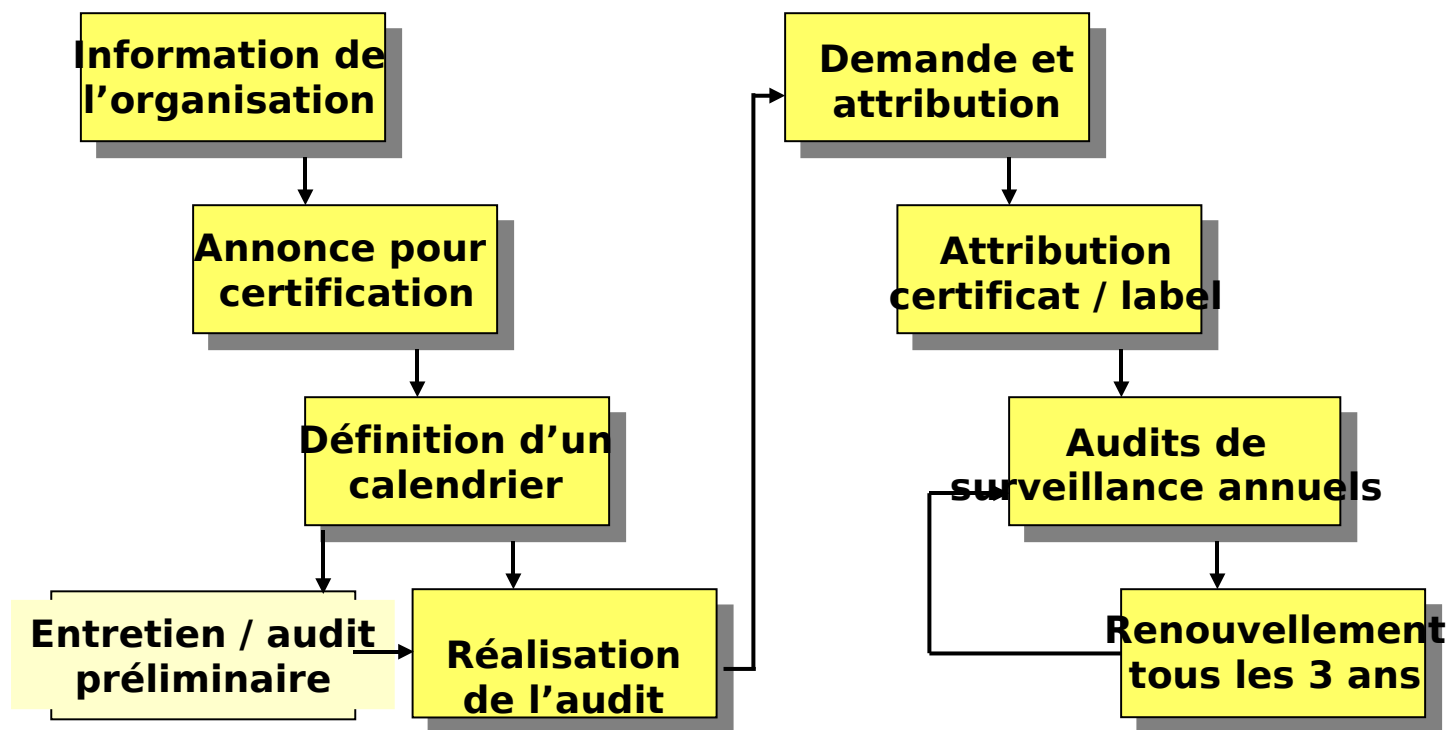
Contenu de l'ISO/IEC 20000-1 (5)

- 1. Management des relations commerciales**
 - Management des relations avec les clients
 - Management des fournisseurs
- 8. Processus de résolution**
 - Management des incidents
 - Management des problèmes
- 9. Processus de contrôle**
 - Management de la configuration
 - Management des modifications
- 10. Processus de mise sur le marché**
 - Management des mises sur le marché

5 étapes pour le succès des projets basés sur l'ISO/IEC20000-1

1. Assurer le management de l'engagement
2. Contrôler la conformité avec l'ISO/IEC20000-1
3. Elaborer un objectif et une stratégie
4. Réaliser / mettre en place
5. Effectuer la certification officielle

Procédure de certification de la SQS



Réalisation de la certification officielle

- Une préparation ciblée et une planification minutieuse conduisent au succès de la certification et permettent l'utilisation de ces logos



Quelques liens

www.isoiec20000certification.com

www.itsmf.org

www.iosm.com

www.sqs.ch