vectis

Serge Raucq

Prolearning SA

Pierre-Paul Boegen

Common Europe Luxembourg
Le 24 mai 2006

Une vue pluridisciplinaire de la conformité

Le gouvernement d'entreprise

Un régime de gouvernement d'entreprise doit reconnaître les droits des différentes parties prenantes à la vie d'une société tels qu'ils sont définis par le droit en vigueur ou par des accords mutuels, et encourager une coopération active entre les sociétés et les différentes parties prenantes pour créer de la richesse et des emplois et assurer la pérennité des entreprises financièrement saines.

(4-ième principe du gouvernement d'entreprise de l'OCDE, 2004)

Les éléments normatifs

Loi du 5 Avril 1993
(Secteur Financier)

Loi du 2 août 2002
(protection données vie privée)

SOX

Contrats

Basle II

EFQM

Périmètre
Normatif

ISO 15504

Cobit

ISO 9001:2000

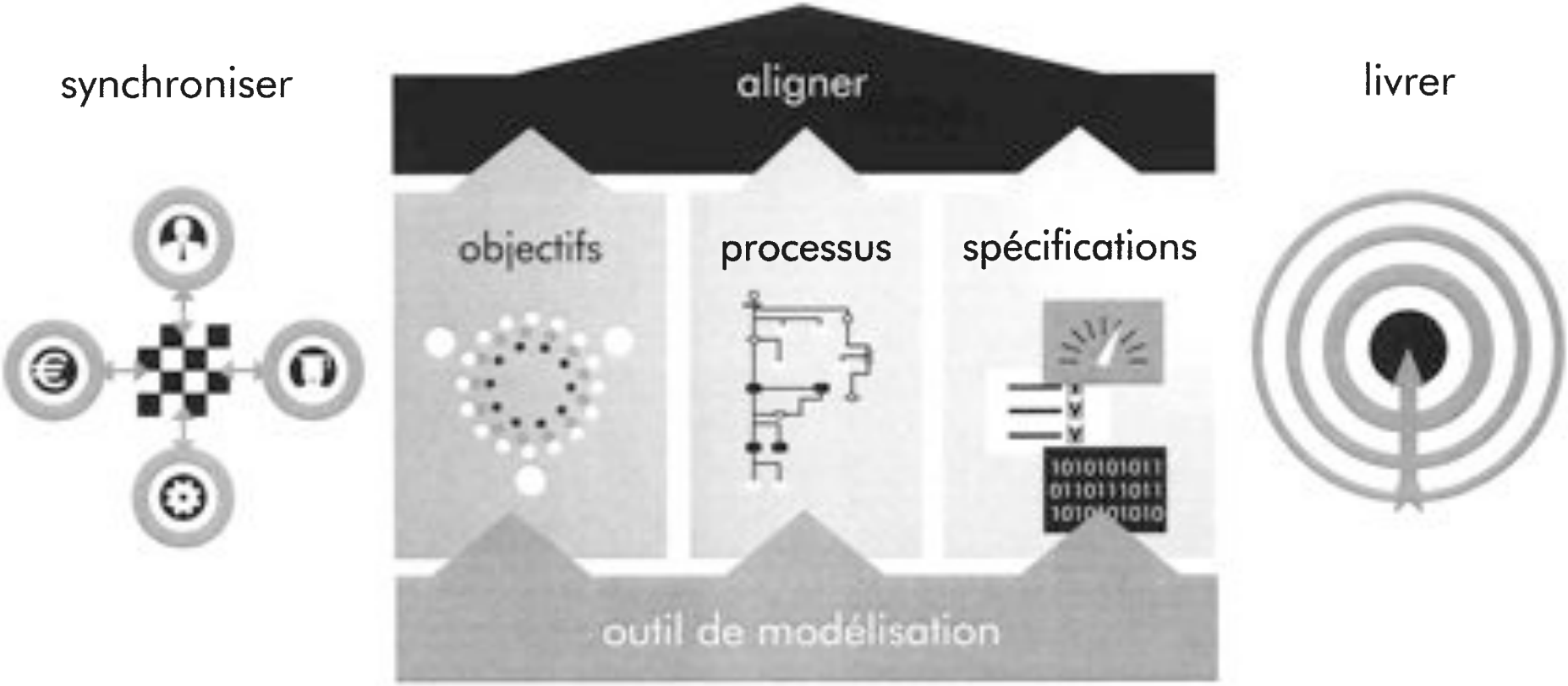
ITIL

CMMI

vectis

Prolearning SA

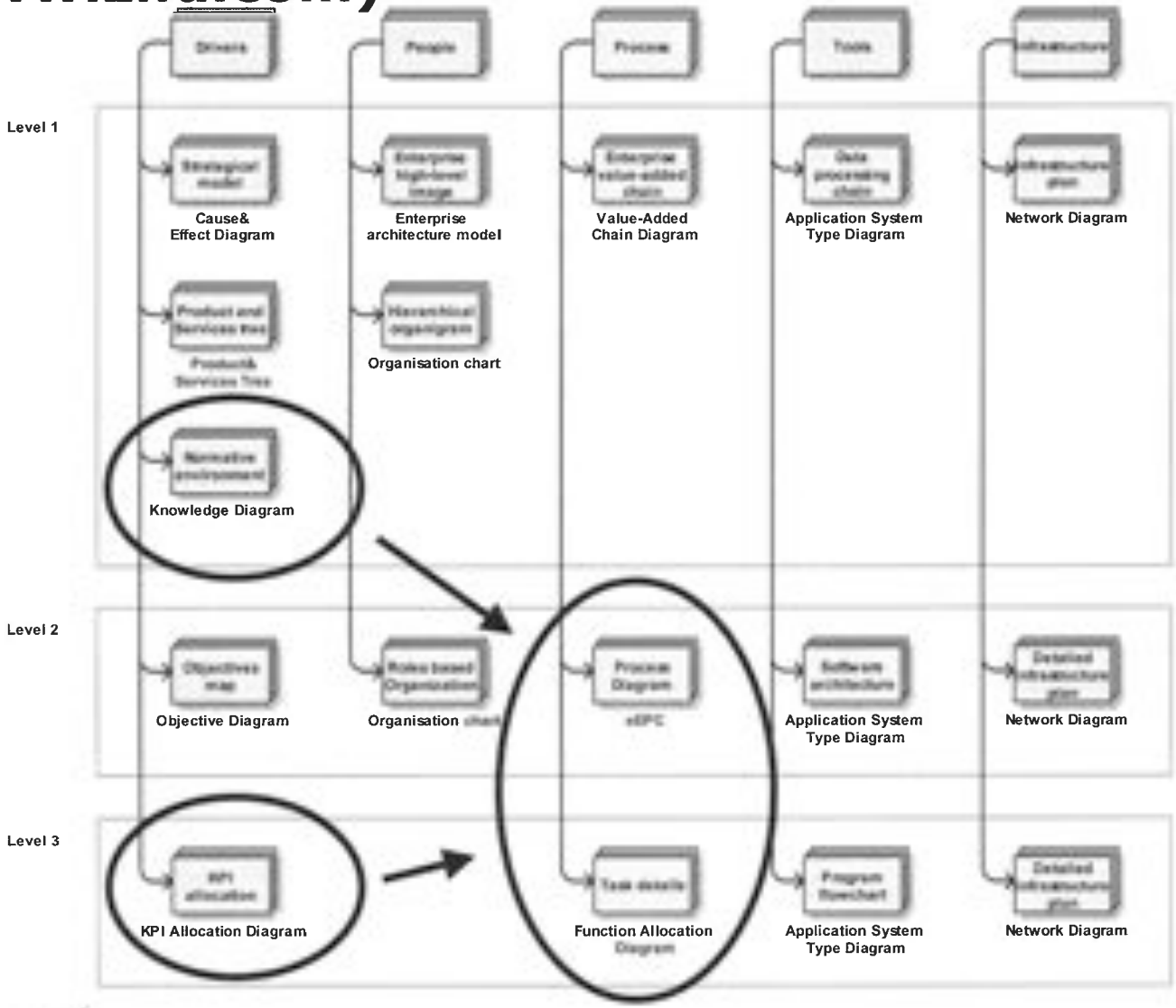
Vue méthodologique



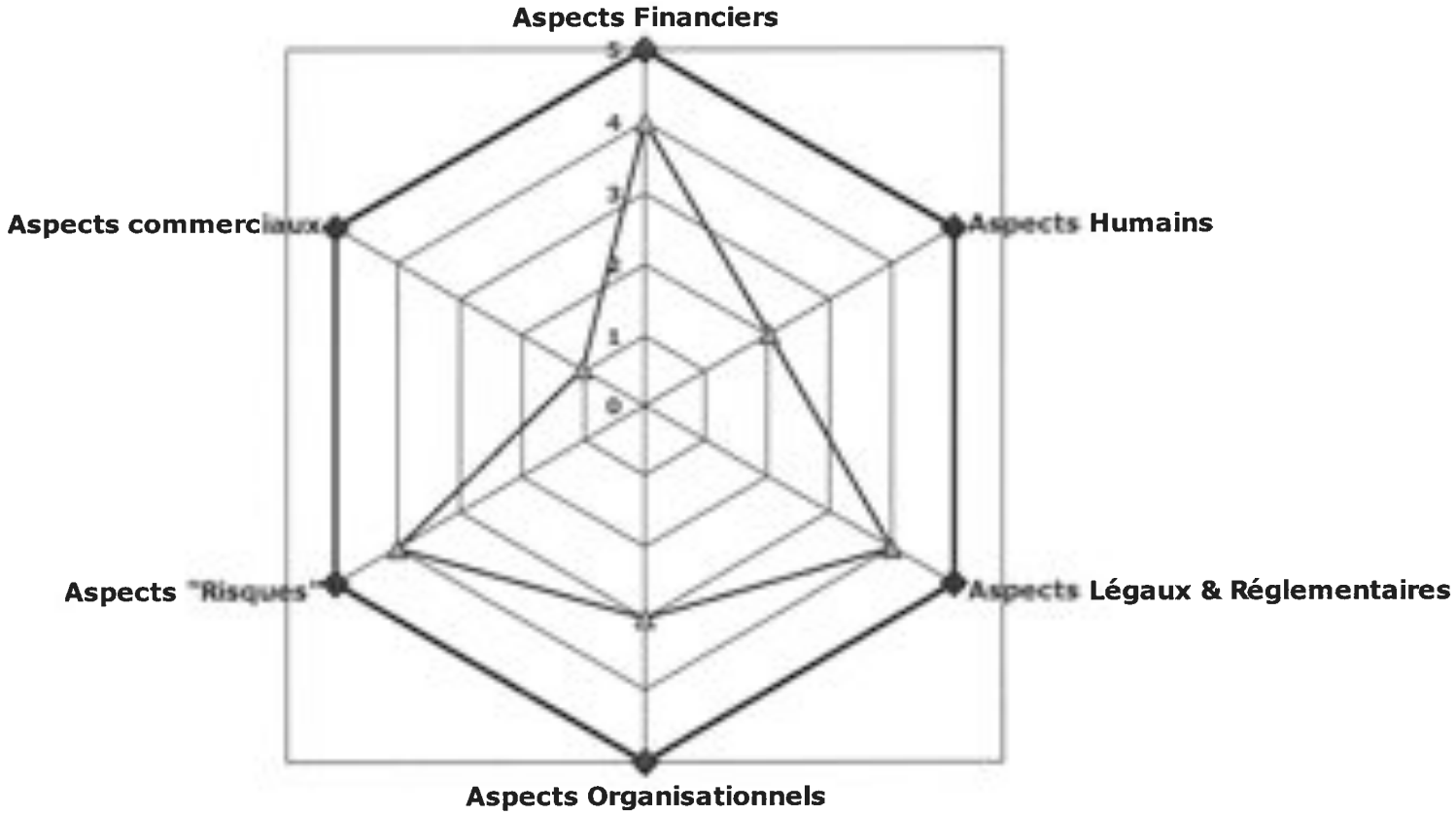
vectis

Prolearning SA

...Inspirée du modèle de Zachmann (www.zifa.com)

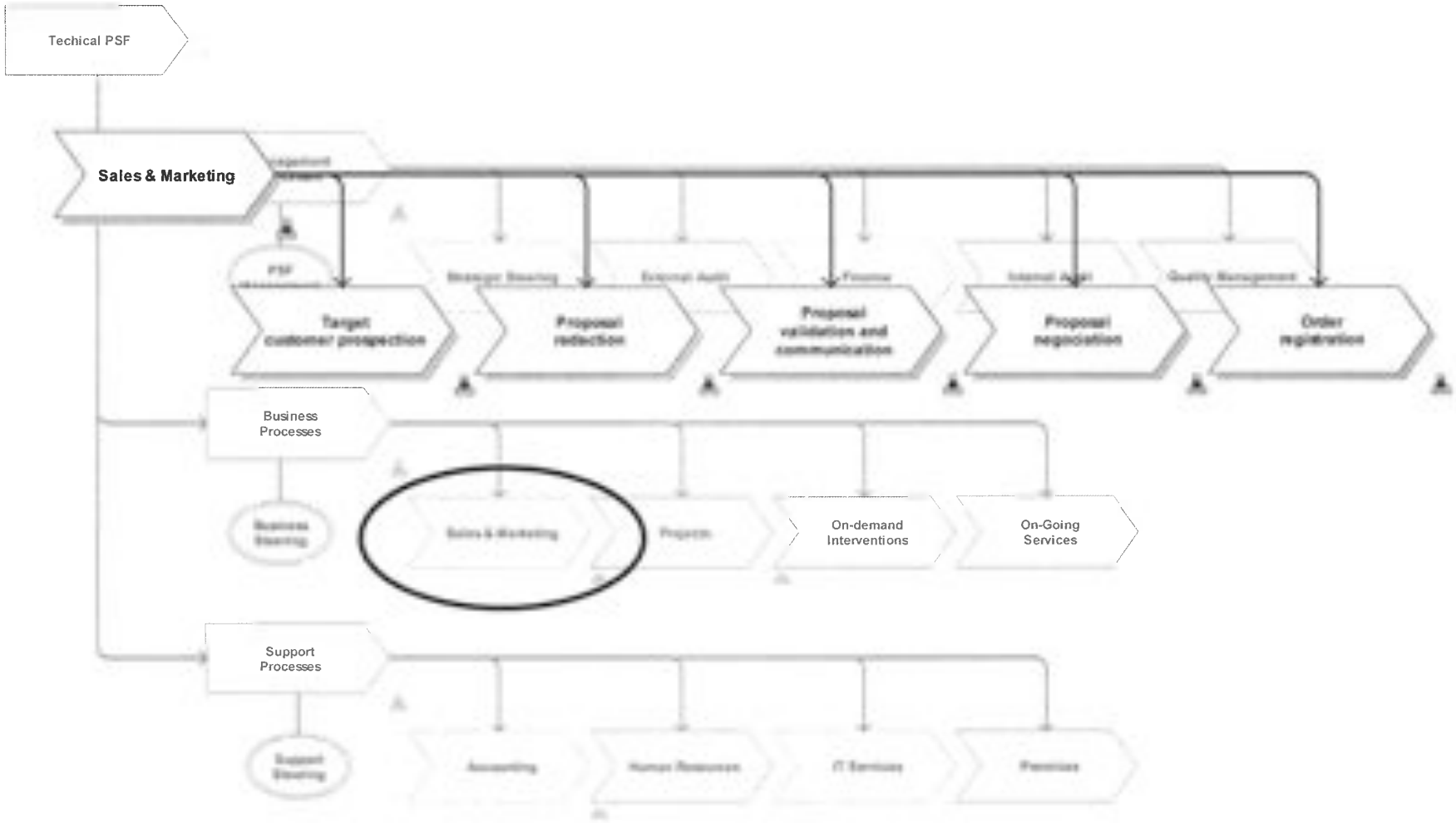


Une approche pluridisciplinaire

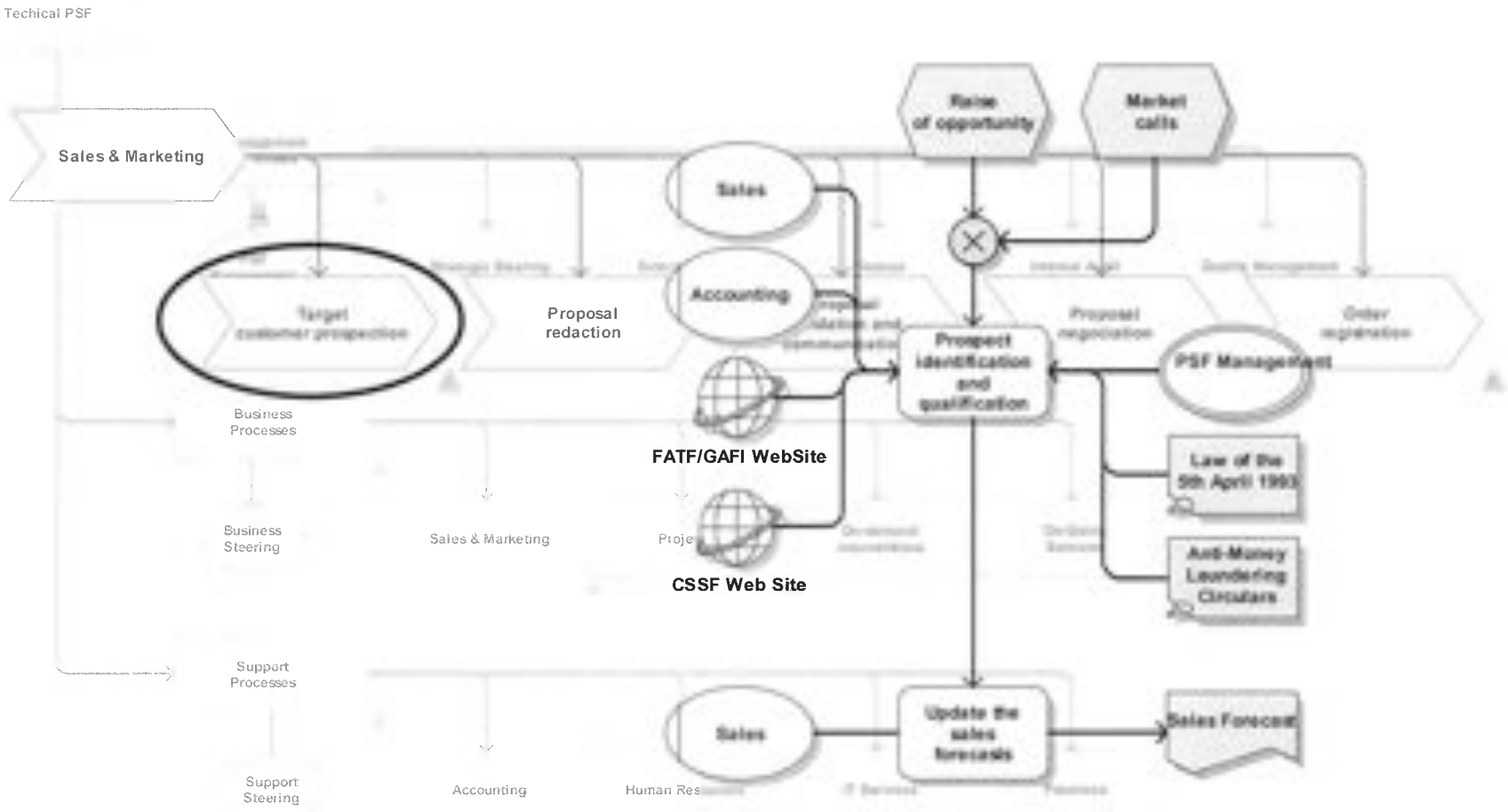


La normalisation d'un processus

La normalisation d'un processus



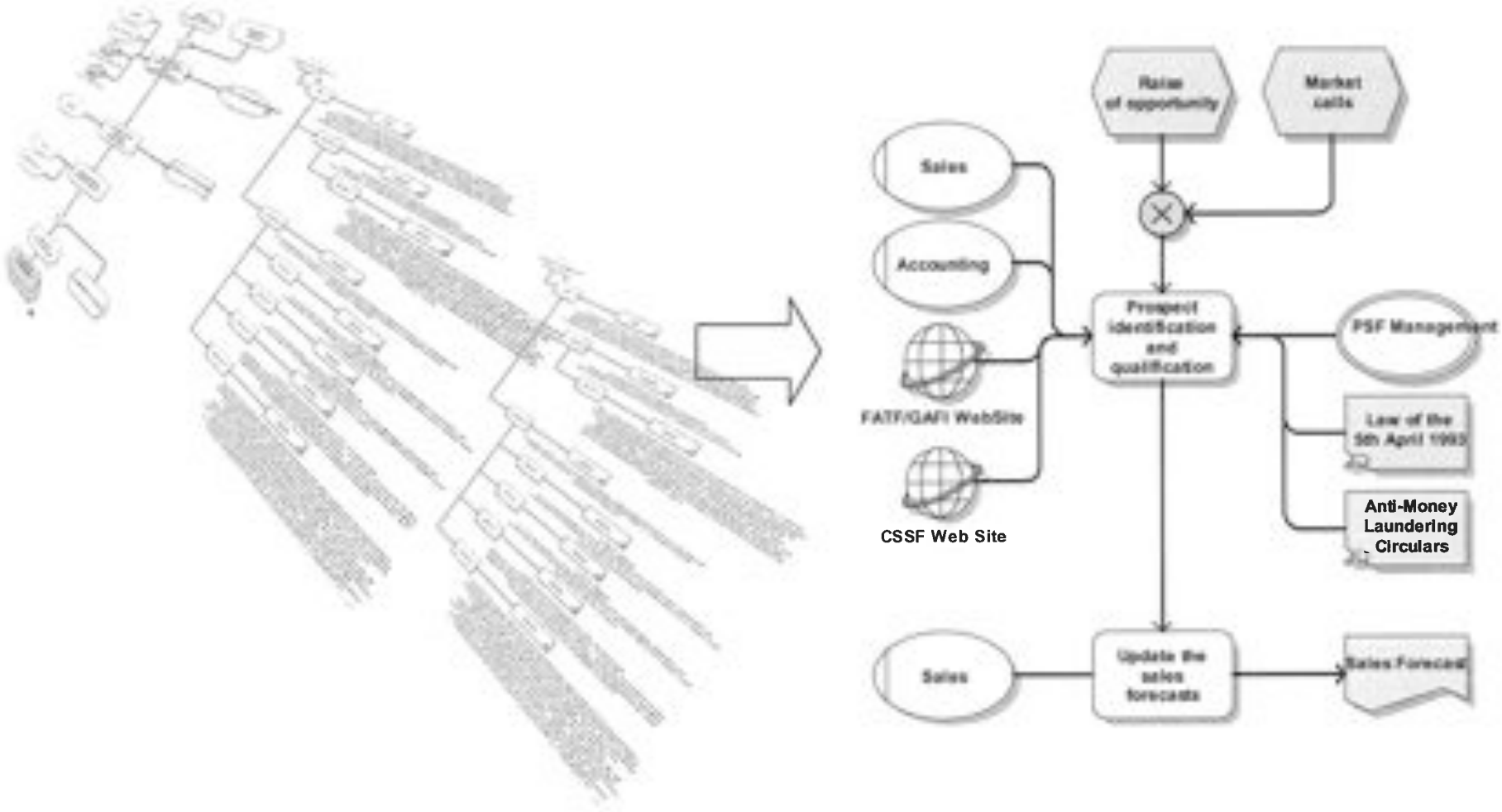
La normalisation d'un processus



vectis

Prolearning SA

La superposition des « Normes »



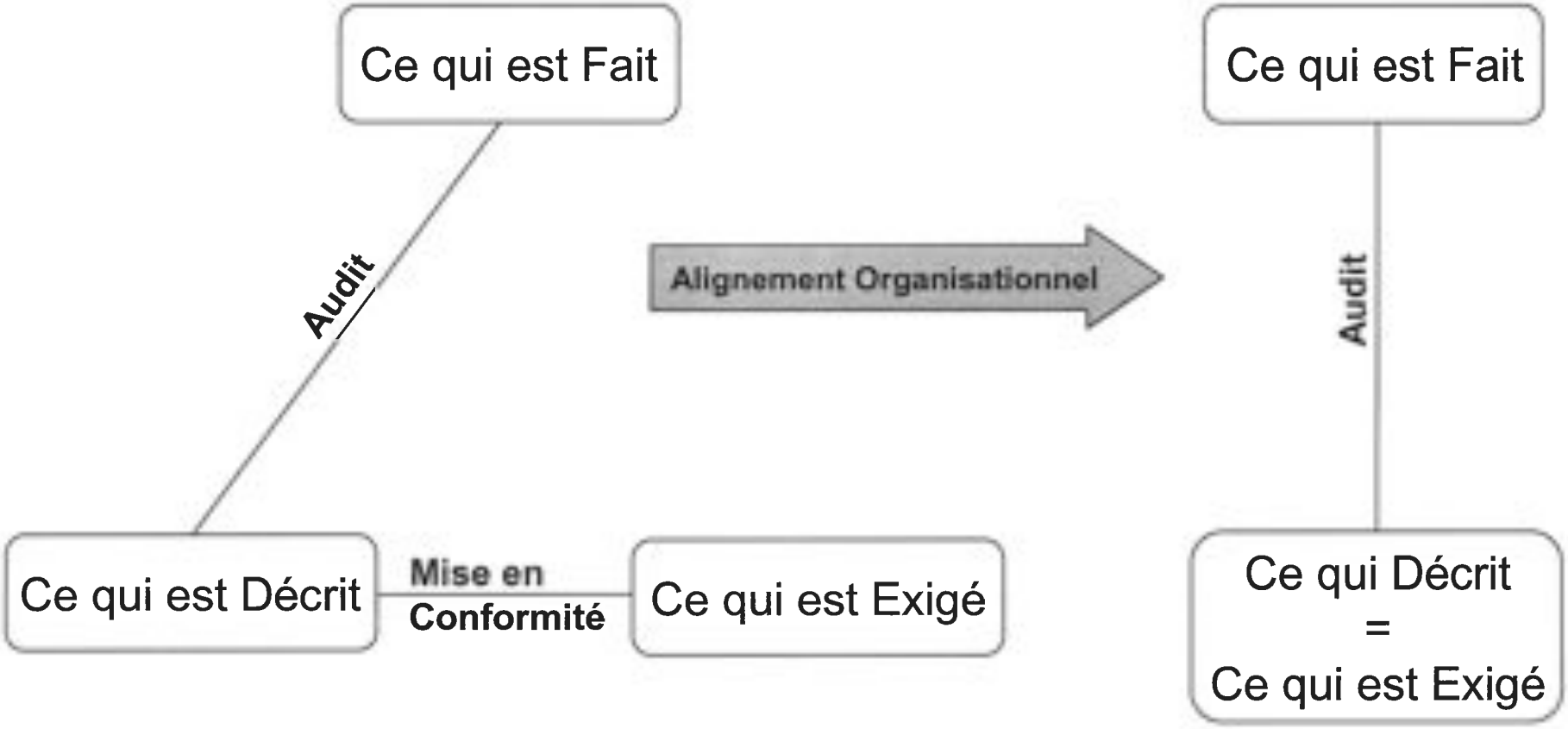
Une matrice de conformité: exemple fictif

Norme / Process	IML 96/126	IML 93/101	ISO 9001:2000	SOX	CSSF 05/211	Loi 5/4/93	...
Vérification Ident. du client	☑			☑	☑	☑	
Signature d'une offre de crédit	☑		☑	☑	☑		
Réception d'un ordre de bourse	☑	☑		☑			
Ident. Contrepartie		☑					
Saisie de l'opération de bourse		☑					
Réconc. Avec un tiers							
...							

Résultats

1. **Mise en perspective des éléments normatifs**
2. **Preuve de niveau de conformité**
3. **Maintenance aisée**
   - En cas de modification des éléments normatifs
   - En cas de modification des éléments normés
4. **Analyse multidimensionnelle des risques**
5. **Diminution des risques opérationnels par**
   - Une meilleure compréhension des processus
   - La mise en valeur du lien « norme - activité »
6. **Forte proximité avec les modèles de maturité**
   - Analyse de maturité facilitée
   - Capacité d'évolution rapide
7. **Homogénéité des représentations organisationnelles**
8. **Facilitation du travail d'audit**

Conclusion: S I M P L I F I C A T I O N



Législation - Réglementation

Toute personne, toute société est soumise aux LOIS du pays.

Qu'il s'agisse du droit pénal, du droit civil, du droit commercial, du droit constitutionnel, etc., chaque citoyen ou résident à des droits mais aussi des devoirs.

La réglementation ne pourra jamais aller à l'encontre des Lois.

Le Secret Professionnel

Loi du 05 avril 1993

Les administrateurs, les membres des organes directeurs et de surveillance, les dirigeants, les employés et les autres personnes qui sont au service des établissements de crédit et des autres PSF ... sont obligés de garder secrets les renseignements confiés à eux dans le cadre de leur activité professionnelle. La révélation de tels renseignements est punie des peines prévues à l'article 458 du CP.

Art. 458 du Code Pénal (16/06/1879)

Les médecins, chirurgiens, officiers de santé, pharmaciens, sages-femmes et **toutes autres personnes** dépositaires, par état ou **par profession**, des secrets qu'on leur confie, qui hors le cas où ils sont appelés à rendre témoignage en justice et celui où la loi les oblige à faire connaître ces secrets, les auront révélés, seront punis d'un emprisonnement de huit jours à six mois et d'une amende de 500 euros à 5 000 euros.

Les sanctions

- Sanctions pénales :
  - ✓huit jours à six mois de prison
  - ✓une amende de 500 à 5 000 euros

- Sanctions civiles : indemniser la personne lésée

Les sanctions

- Sanctions indirectes :

  la réputation du PSF,

  la réputation de l'employé,

  la transmission d'informations à l'étranger et ses conséquences, etc.

- Sanctions sociales : licenciement de l'employé

Le secret professionnel

Le secret professionnel est l'obligation pour tout un chacun qui est lié à un établissement de crédit ou à un PSF de garder secrets les renseignements confiés à lui dans le cadre de son activité professionnelle.

Le Secret Professionnel

Les personnes concernées

Les limites dans le temps

Les limites dans l'espace

Les limites du secret professionnel

- la sphère de discrétion (client, mandataire, etc.)
- les autorités (CSSF, réviseurs, etc.)
- les autorités judiciaires (AML, abus de marché, partie ou témoin à un procès, entraide judiciaire, etc.)
- les actionnaires (sous certaines conditions)

Préservation des données confidentielles

Les données confidentielles

- LES INFORMATIONS CONCERNANT LE CLIENT
- LE « KNOW HOW »

Préservation des données confidentielles

La perte de ses données

Fuite interne, externe, des fraudes, négligences, etc.

Les activités à risque

Toutes les activités

Les prestataires externes

Tous les prestataires

Des négligences internes

- Les documents non rangés, oubliés, emportés
- Les armoires, bureaux, etc. non fermés à clef
- Les poubelles contenant des documents non détruits
- Les sous-mains « cachant » des informations
- Les archives, bandes magnétiques, …mal sécurisées

Des négligences externes

- Les documents perdus, oubliés, volés, etc. dans un lieu public
- Les conversations, bavardages
- Où ? tout lieu public
- Les travaux à domicile volés, perdus, saisis
- Le GSM (en public, photos, connexion internet, etc.)

Préservation des données confidentielles

QUATRE MESURES INDISPENSABLES :

1) respecter les procédures, un code de déontologie, une Charte de sécurité des données confidentielles
2) signaler les risques de perte de données (nouveaux risques, risques non couverts actuellement par les procédures, etc.)
3) « need to know »
4) contrôler le respect des procédures

Préservation des données confidentielles

D'AUTRES MESURES :

- Une destruction **totale** des documents
- Une conservation **securisée** des documents et un accès au archive **restreint**
- Pour l'échange, la cession ou la vente de matériel, **s'assurer** que ce matériel ne « contient » plus d'informations
- Pour l'organisation du PSF :

  la conception des locaux : prendre en compte la sécurité des données (insonorisation, discrétion à la réception, orientation des écrans, etc.)

Préservation des données confidentielles

D'AUTRES MESURES :

- Pour le personnel :

  - « need to know »
  - « clean desk »
  - rangement
  - armoires, tiroirs, coffres, … fermés à clef
  - destruction correcte des documents
  - vigilance à l'intérieur et à l'extérieur (conversation entre collègues, confrères, conjoint, au téléphone, au GSM, etc.)

Préservation des données confidentielles

L'INFORMATIQUE

Des principes généraux

- La **confidentialité** de l'information
  - ✓ seulement au personnel autorisé
- L'**intégrité** de l'information
  - ✓ information correcte, complète, fiable
- La **disponibilité** de l'information
  - ✓ en permanence et sans possibilité de fraude
- Les **preuves et contrôles**
  - ✓ assurer la trace de l'origine, du traitement, de la consultation, … des informations

Préservation des données confidentielles

L'INFORMATIQUE

Des principes généraux

- **Accès** limité pour les locaux de l'informatique
- **Séparation** entre développement et production
- Instaurer une **politique de sécurité** pour :

  les back up, la production des copies papier, l'archivage, l'échange du matériel, etc.
- Documenter et autoriser toutes **les exceptions**

L'accès aux applications informatiques

Le mot de passe :

Les raisons d'une communication volontaire :

- pour faciliter le travail
- pour aider en cas d'absence, etc.

Les conséquences :

- responsabilité en cas d'erreur, en cas d'usage abusif
- responsabilité en cas d'indiscrétion professionnelle, de fuite d'informations confidentielles, de vol de données

L'accès aux applications informatiques

Le mot de passe :

Les causes d'une communication involontaire :

- fraude, « hacking », etc.
- négligences

Les conséquences :

- permettre la fuite du mot de passe
- permettre l'accès à ses applications informatiques
- etc.

L'accès aux applications informatiques

Le mot de passe :

Des négligences :

- le mot de passe transcrit sous le clavier, le sous-main, dans son portefeuille, sous le tapis de souris, le post it collé sur l'écran, etc.

- le mot de passe trop simple, trop court : Tintin, Stippy, coucou, etc.

- un script (saisie du mot de passe automatisée)

Préservation des données confidentielles

Internet - Intranet

Des risques de perte (fraudes, négligences, erreurs)

- ✓adresse erronée dans l'envoi
- ✓ liste des destinataires non à jour
- ✓ « attachment » incorrect

Des risques légaux

- ✓ que diffusons-nous ?
- ✓ à qui ?

Protection des données... et vie privée

Protection des données... et vie privée

La législation :

- Loi du 02 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- Règlement grand-ducal du 27 novembre 2004 concernant le chargé de la protection des données
- Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques

Protection des données... et vie privée

Donnée à caractère personnel :

Toute information concernant une personne identifiée ou identifiable.

Toute personne (physique ou morale) est identifiable par un numéro d'identification ou par un ou des éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

Protection des données... et vie privée

Le traitement de données à caractère personnel :

Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données.

Il s'agit de la collecte, de l'enregistrement, de l'organisation, de la conservation, de l'adaptation ou de la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, de la diffusion ou toute forme de mise à disposition de données, du rapprochement ou de l'interconnexion ainsi que du verrouillage, de l'effacement ou de la destruction de données.

Protection des données... et vie privée

10 commandements :

1. Principe de légitimité : avoir l'accord, quand et comment ?
2. Principe de finalité : pourquoi détenir ces données
3. Principes de nécessité et de proportionnalité : limiter les données
4. Principe d'exactitude : données correctes, actuelles
5. Principe de loyauté : de bonne foi, pas à votre insu
6. Principe de sécurité et de confidentialité : le traitement, la conservation
7. Principe de transparence : contrôle personnel

Protection des données... et vie privée

10 commandements :

8. Certaines données sont soumises à une protection encore renforcée : opinions, convictions, état de santé
9. La surveillance de personnes identifiables est strictement limité
10. Utilisation de données à des fins de publicité, démarche commerciale est soumise à autorisation expresse

Protection des données… et vie privée

Les droits :

1. Droit à l'information
2. Droit d'accès à vos informations personnelles
3. Droit de vous opposer au traitement de vos données personnelles
4. Droit d'information sur des processus de décision automatisés

Protection des données... et vie privée

Faire valoir ses droits :

1.Consultation du registre public :

La Commission Nationale pour la Protection des Données (CNPD) a établi un registre public des traitements accessible sur Internet.

2. Réclamation directe :

Demander à qui détient l'information sa finalité

3. Plainte auprès de la CNPD

4. Saisine du Tribunal

La déontologie

La déontologie

Pourquoi ?

1. Respect des lois & règlements

• conduire l'activité journalière envers la clientèle avec une éthique irréprochable

• dans le travail quotidien

• dans l'observance de l'esprit des lois. Ne pas chercher à les éviter, à les détourner

La déontologie

Pourquoi ?

2. Respect des principes de base

- établir une confiance
- avant tout servir le client
- avoir une gestion sérieuse et transparente
- observation stricte des lois, règlements et codes internes
- respect du droit de l'homme et de l'environnement
- désaveu des violations de l'ordre public

Pourquoi ?

3. Respect de la confidentialité & de la discrétion

- rappeler le secret professionnel
- organiser des règles générales qui impose la confidentialité
- disposer de l'information utile et nécessaire

Pourquoi ?

4. Devoirs et qualités de la relation avec le client

- le connaître
- lui fournir une information appropriée
- le servir avec diligence et loyauté
- écarter les conflits d'intérêts
- ne pas l'inciter à des infractions
- garder son indépendance à son égard

Pourquoi ?

5. Devoirs d'honnêteté et d'intégrité

- honnête envers soi-même permet le respect des devoirs envers l'entreprise, le client, les collègues

En résumé

1. Le comportement envers les clients, les marchés, les contreparties

- confidentialité
- connaissance du client
- qualité du conseil
- pas de conflits d'intérêts
- connaissance et acceptation du « vrai » cadeau d'usage
- respect des déontologies spécifiques

En résumé

2. Le comportement envers l'établissement

- loyauté
- honnêteté
- respect des procédures
- comportement hors de l'établissement
- souci de la sécurité
- accord pour l'exercice d'une autre activité

En résumé

3. <u>Le comportement envers les collègues</u>

- solidarité, compétence, honnêteté
- non-discrimination

4. <u>Le comportement envers la Loi et les autorités</u>

- connaissance des Lois et règles
- collaboration avec les autorités

SOX

Une vue d'ensemble

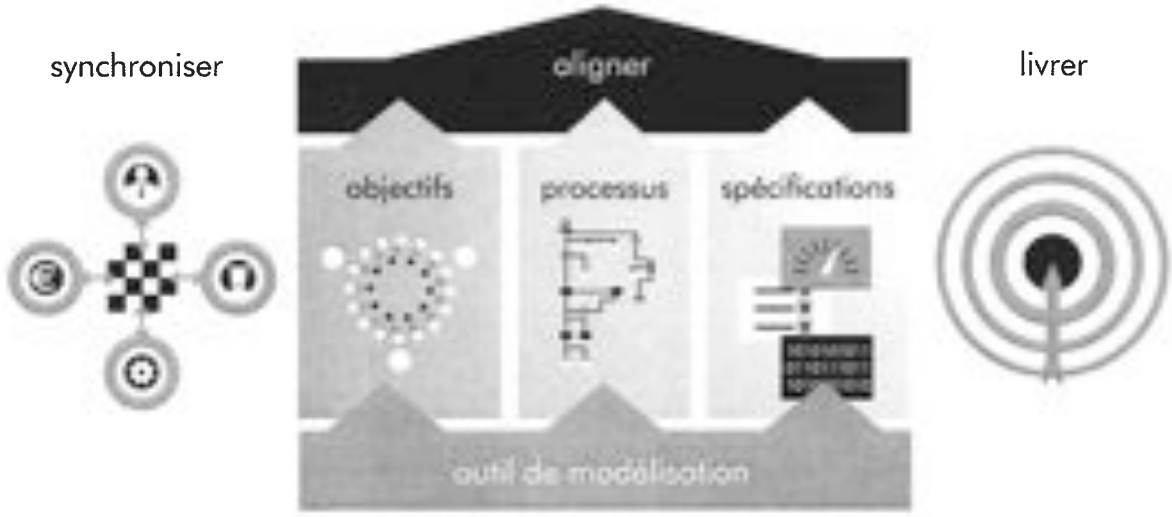
Sarbanes Oxley Act Overview

Areas of emphasis	Management Reporting	Board Governance	Management & Board Conduct	Enforcement & Penalties	Auditor Independence
Key Sections	Management Reporting	Board Governance	Accelerated reporting of insider trading	Public Company Oversight Board (PCAOB)	Audit Commitee pre-approval all auditor services
	Management Report on Internal Controls	Prohibition of loans to Directors & Officers	Disclose Code of conduct for finance officers	Criminal penalties for knowingly untrue certifications	Prohibits auditor from certain services
			Protection of whistleblowers		Lead audit partner limited to 5 years rotation

Constatation

1. **Les contraintes sont proches des requêtes CSSF**
   Beaucoup de recoupements
   Quelques différences facilement mises en lumière

2. **La mise en conformité suit le même schéma**



Exemple: SOX section 404 vs. IML 98/143

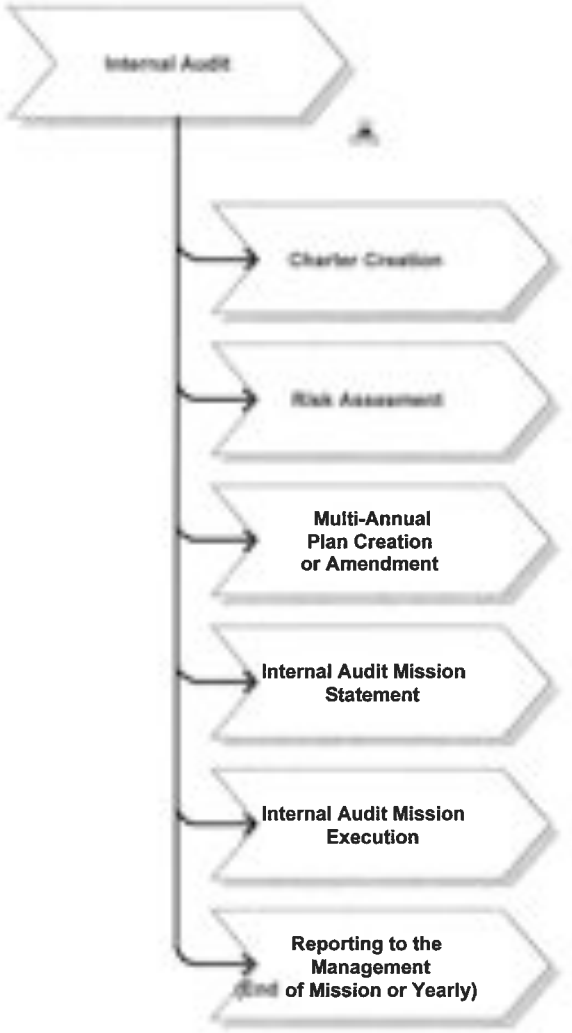
■ Responsabilités du management

Effective Year End 2004 CEO & CFO must include a report in the Annual Report indicating:

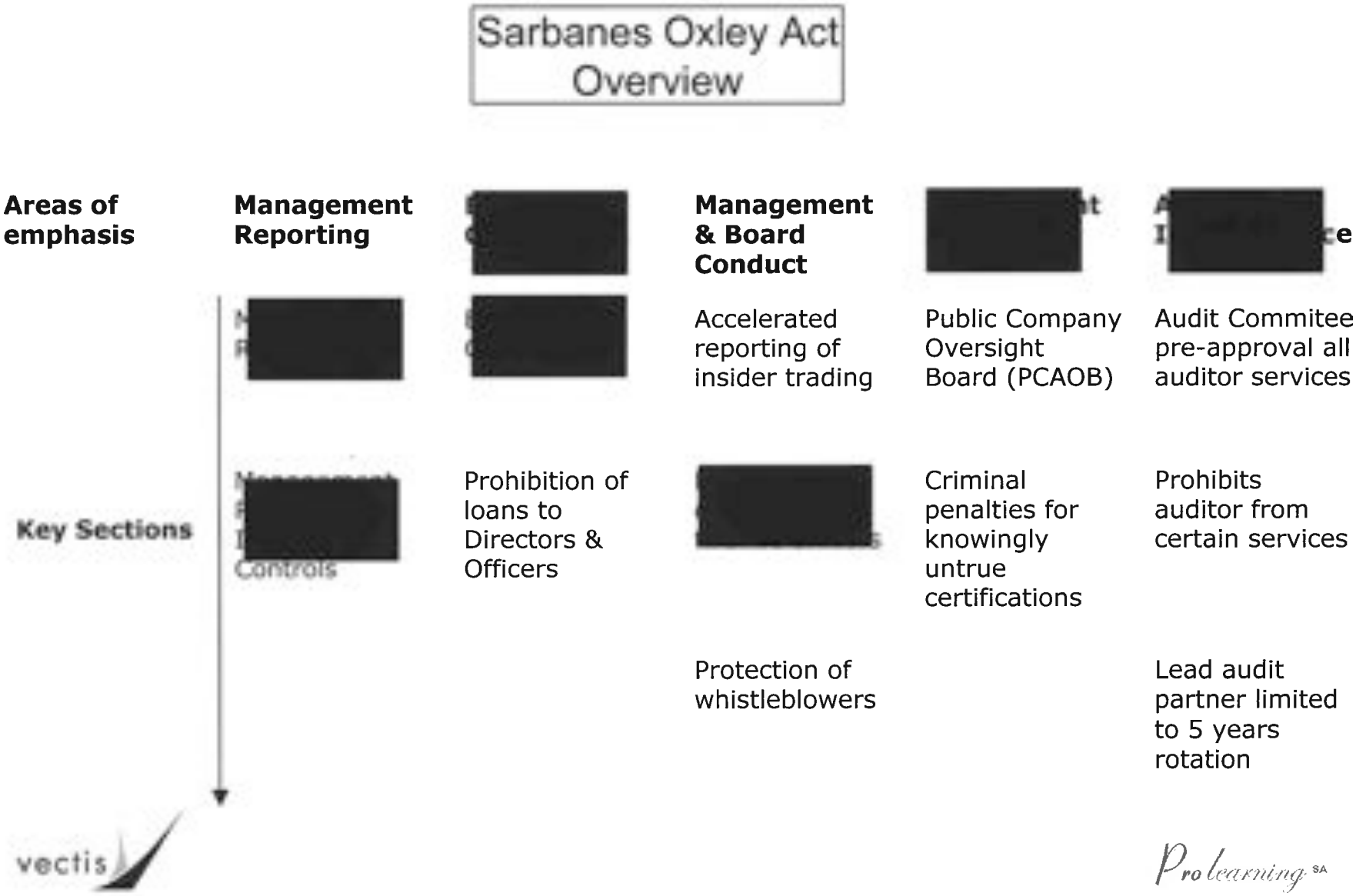
1. They have designed and maintained a system of internal controls for financial reporting using a recognized internal control framework
2. They have tested internal controls and found them to be designed and operating effectively
   The Auditor has evaluated the design and effectiveness of the controls and found them to be operating effectively
3. Effective Q1 2005, CEO and CFO must certify quarterly that there are no significant changes to internal controls for financial reporting using a recognized internal control framework.

IML 98/143 vs. SOX section 404

1. Contrôle interne
2. Rôle de la direction
3. Reporting à la CSSF
4. … déjà en 1998



Une vue d'ensemble... mais plus (exemples)



Des différences quand même

1. **SOX met le Conseil d'Administration au centre de l'entreprise**

2. **Les circulaires de la CSSF mettent l'organisation au centre de l'entreprise**

   Universalité des responsabilités

Bâle II ... et ISO 15504

Bâle II: définition des risques opérationnels

1. Risques opérationnels(*)

   Les principales catégories de risques opérationnels sont liées à des **carences** dans les **contrôles internes** et la **gouvernance d'entreprise**. Celles-ci peuvent entraîner des pertes financières par suite d'**erreurs**, de **fraudes** ou de **l'incapacité de s'exécuter à temps**, ou nuire d'autre manière aux intérêts de la banque, notamment parce que ses opérateurs, responsables des prêts ou autres agents auront **outrepassé leurs pouvoirs** ou effectué leur activité sans respecter les **principes de déontologie** ou de **prudence**. D'autres aspects du risque opérationnel résident dans de **graves défaillances des systèmes d'information** ou dans des événements tels qu'un gros incendie ou un désastre.

(*) www.bis.org

Le modèle de maturité ISO 15504

1. **Méta-Norme**

   Structure formalisée dédié à la gestion des exigences d'un processus

2. **Contient:**

   Un modèle de management de processus

   Un ensemble cohérent d'exigences et de guides concernant:

   - L'évaluation et
   - L'amélioration des processus

Les 6 niveaux de maturité d'ISO 15504

Niv	Définition d'origine	Traduction	Concepts
0	***Not-Performed***	Non effectué	Mise en œuvre de pratiques empiriques
1	***Performed-Informally***	Effectué de façon informelle	Mise en œuvre de pratiques définies
2	***Planned-and-Tracked***	Planifié et Suivi	Planifier des procédures définies, ordonnancer, puis suivre leur exécution
3	***Well-Defined***	Bien défini	Définir un processus formalisé et standardisé, puis le mettre systématiquement en œuvre
4	***Quantitatively-Controlled***	Maîtrisé quantitativement	Établir des objectifs-qualité mesurables, mettre en place des indicateurs, puis piloter leur suivi
5	***Continuously-Improving***	En amélioration permanente	Améliorer les pratiques organisationnelles et accroître l'efficience du processus

Bâle II et l'externalisation

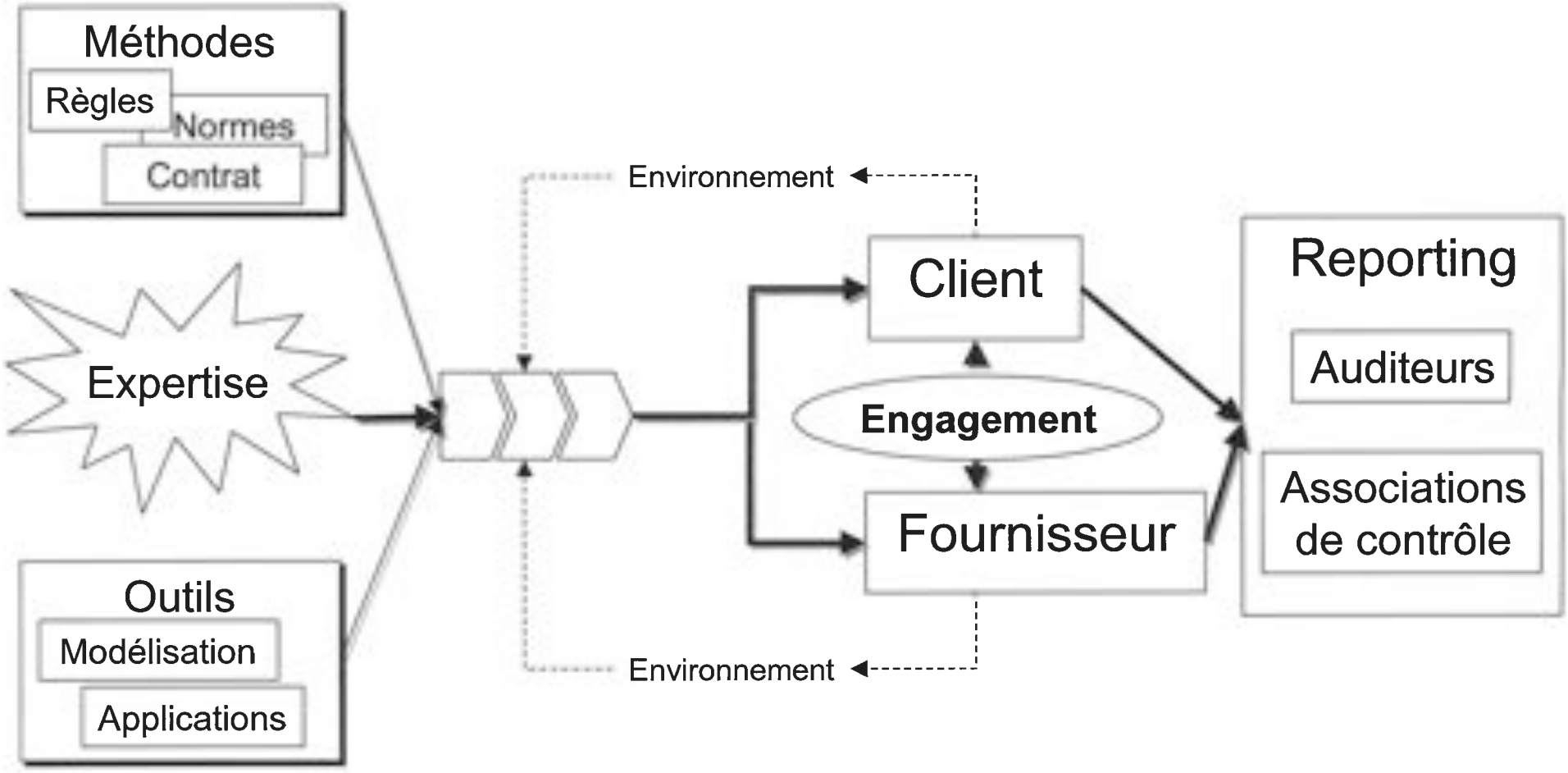
1. **Proximité des besoins d'évaluation**
   Basle II vs. ISO 15504

2. **Intérêt du régulateur sur le modèle de maturité**
   Cfr. Projet « Grif »

3. **Proximité CSSF 05/178 (entre autres…)**
   Par ailleurs, le professionnel financier doit être en mesure de fonctionner normalement en cas de panne de son système informatique et il élaborera à cet effet une solution de «back-up» en adéquation avec un plan de continuité des activités. Le **plan de continuité** vise à décrire les actions à mettre en œuvre afin de poursuivre les activités en cas d'incident ou sinistre lié à des événements anormaux.

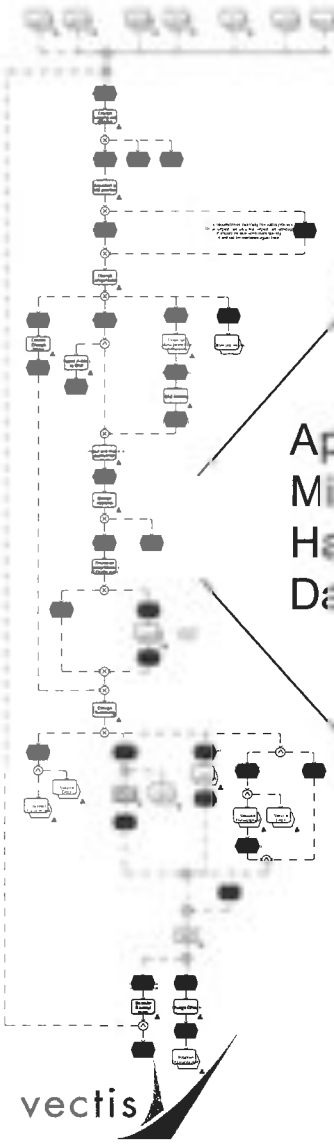
ITIL

Un cas pratique: ITIL

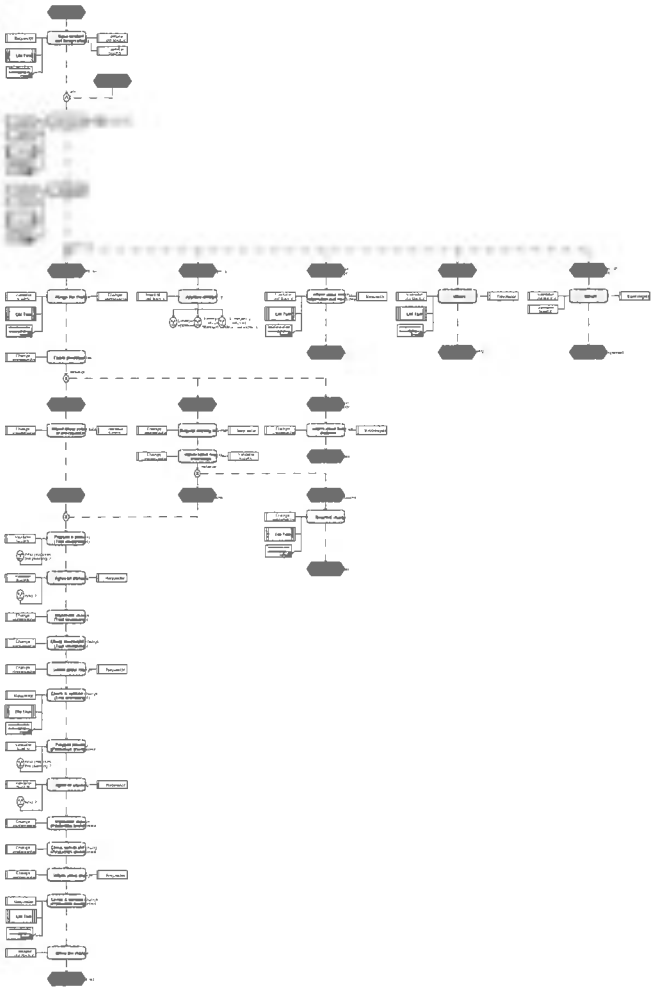


Exemple: Change Management

ITIL Change Reference



Customisation du Change



- CI (Config. Items)
- Outil de suivi
- Procédures opérationnelles associées

Matrice

RFC	CI 1	CI 2	CI 3
Op 1			
Op 2			
Op 3			

ITIL… et SLA

1. **Syndrôme de la « page blanche »**

2. **« Je n'externalise que ce que je maîtrise… »**

3. **« Externaliser un processus, ce n'est pas l'éliminer ».**

Conclusions

Soumis ou non à une législation particulière, à des règlements, à une déontologie (volontaire ou imposée) :

LA SÉCURITÉ DES DONNEES N'EST-ELLE PAS NOTRE PREMIER SERVICE AU CLIENT ?

En respectant lois, réglementations et meilleures pratiques:

nous oeuvrons pour l'image de marque de notre établissement, donc son développement, ses emplois, sa sécurité.