



Telindus Arche

France Telecom
Yves LECLERQ

Jean Marc CHARTRES

EDF :



Il n'y a pas de progrès sans risque

- 15 grands assureurs et réassureurs européens ont **perdu jusqu'à deux tiers de leurs fonds propres !** (Aegon, AGF, Allianz, Aviva (CGNU), AXA, Baloise, Generali, ING, Munich Re, RAS, Royal & Sun, Alliance, Sampo, SCOR, Swiss Re, Zurich Financial)
- La valeur de marché de ces 15 sociétés est passée de **607 milliards € à 237 milliards €!**
 - Il en a résulté une **perte de capitaux** s'élevant à 370 000 000 000 €
- Inculquer une **culture de risque** au sein de l'entreprise
 - Chaque collaborateur est gestionnaire de risque
- Satisfaire aux exigences légales en la matière
 - Ce ne sont pas des contraintes, mais des règles de base

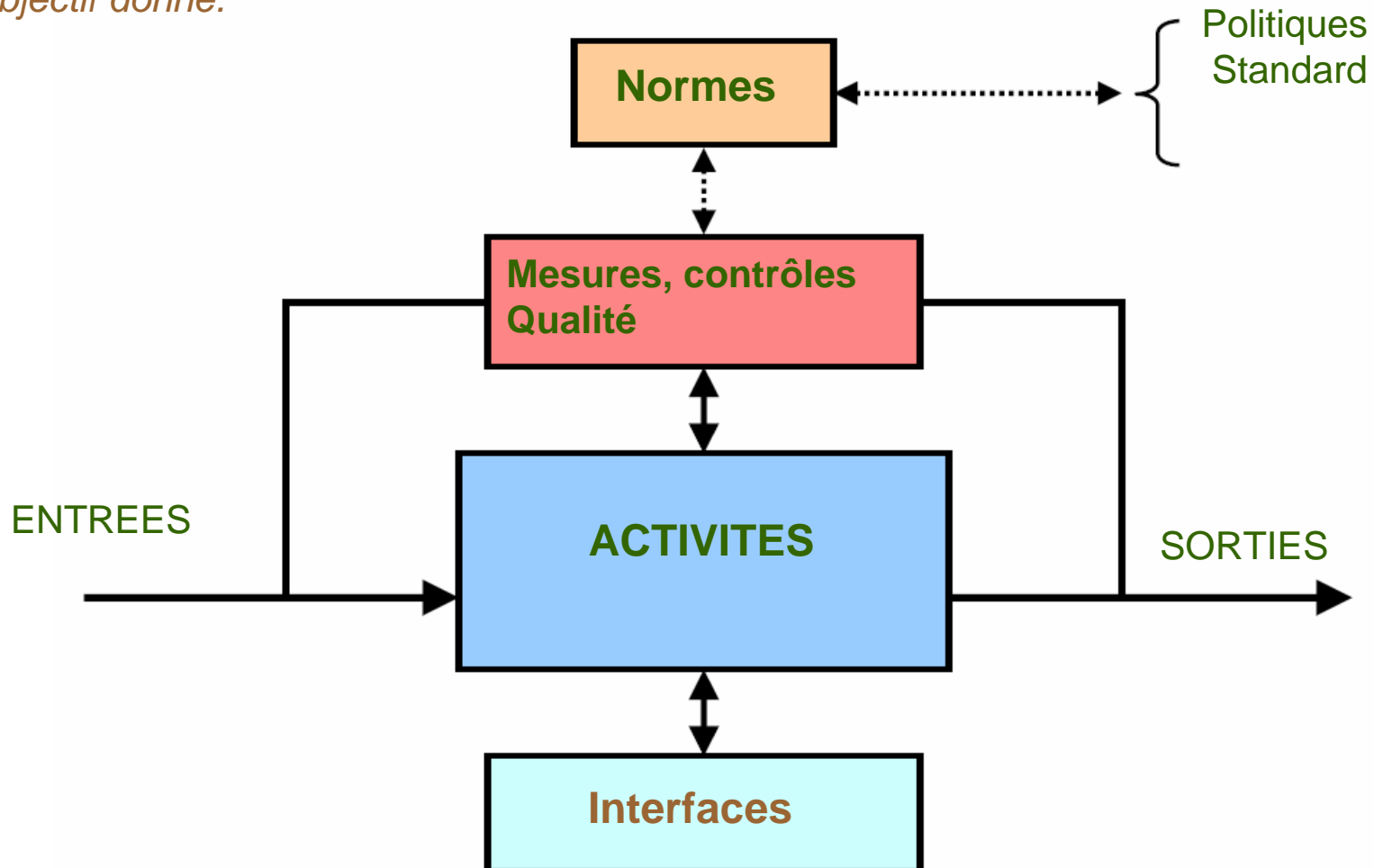
« Nous faisons face à l'émergence d'un nouvel univers des risques... qui va conduire à transformer en profondeur le comportement des divers acteurs concernés et à modifier le fonctionnement et la formation des équilibres des marchés de transfert de risques »

Denis Kessler Amrae 2004



Processus SI

❖ *Un processus est un ensemble **d'activités, de pratiques, d'outils, d'équipements et de méthodes** que des personnes formées mettent en oeuvre pour atteindre un objectif donné.*



- Condamne le « **Manquement à la Sécurité** »
 - Si rien n'est fait pour atteindre le risque résiduel
- Protège le **droit privé** et les libertés individuelles
 - Avec loyauté et transparence
 - Et encadre le contrôle et la surveillance
- Condamne le « **délit informatique** »
 - Difficultés : Délit immatériel (preuve, évaluation, auteur, .)
- Protège le **patrimoine informationnel**
 - Personnes, Biens, Connaissances (Actifs)



- **Audit et enregistrement :**
 - Analyse des traitements mis en oeuvre par le responsable et non soumis à autorisation préalable et tenue d'un relevé afférent
- **Contrôle et surveillance des traitements :**
 - Assurer de manière indépendante le respect de la législation par le responsable de traitements qui l'a désigné
 - En cas de doute quant à la conformité d'un traitement, il doit consulter la Commission nationale et éventuellement informer la Commission nationale de toute irrégularité constatée dans les traitements qu'il surveille et à laquelle le responsable du traitement n'a pas remédié
- **Interface entre la Commission nationale et le responsable de traitement**
- **Conseiller avec rôle d'alerte et de recommandation:**
 - informer le responsable du traitement sur les formalités à accomplir mais aussi sur les autres obligations légales et les droits des personnes concernées
 - suggérer des améliorations, initiatives d'autodiscipline (code de conduite)
 - contribuer à la sensibilisation et à l'information du personnel
- **Investigateur et médiateur**
 - dans l'intérêt de la protection de la vie privée des personnes concernées (clients effectifs ou potentiels, fournisseurs, affiliés, salariés, administrés, patients, ...) et du respect de leurs droits individuels

Les administrateurs systèmes et réseaux

- Chargés de la mise en œuvre et de la surveillance des systèmes et du réseau. A ce titre, ils gèrent les traces
- Chargés de rapporter toute anomalie de fonctionnement
- Tenus au secret professionnel et ne répondent, sauf réquisition de l'autorité judiciaire, à aucune autre demande d'information ou de traitement pouvant mettre en cause des personnes ou porter atteinte à leur vie privée
- Doivent donner acte, par la signature d'une déclaration d'engagement qu'ils ont été informés

Le projet de loi de lutte contre le terrorisme

a été approuvé mardi 29 novembre 2005 à l'Assemblée nationale .

Il prévoit l'obligation de conserver les données de connexion des clients, appelées "logs", des opérateurs télécoms, des fournisseurs d'accès internet, mais aussi des cybercafés, pendant une durée maximale d'un an.

Un décret d'application devra ensuite préciser la nature exacte des données et la durée de conservation suivant les cas.

- **Une loi répond à des exigences impérieuses**

- Se situe au coeur des processus métiers des entreprises.
- Suit des cycles technologiques extrêmement rapides.
- Conquiert continuellement de nouveaux espaces.

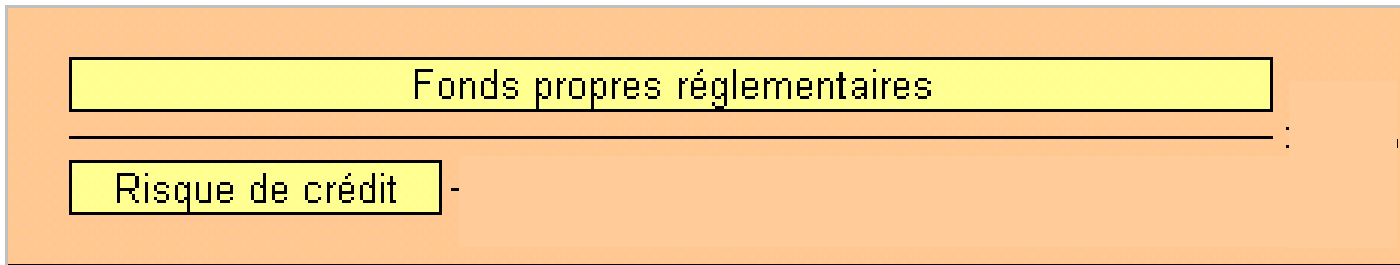
Loi sur la Sécurité Financière (LSF)

- La LSF a été votée par le parlement français en août 2003, Cette loi vise à améliorer la qualité de l'information fournie aux actionnaires et au public, renforcer la responsabilité des dirigeants dans l'élaboration des rapports d'activités, ainsi qu'à augmenter la fiabilité de ces rapports.
- Pour cela, les dirigeants des Sociétés Anonymes doivent rendre compte des procédures de contrôle interne dans le rapport annuel. De même, les commissaires aux comptes doivent auditer les procédures de contrôle interne "relatives à l'élaboration et au traitement de l'information comptable et financière" et inclure leurs conclusions dans le rapport d'activité. La fiabilité du processus de consolidation des données comptables et financières est au coeur de ces nouvelles dispositions.

Contraintes métiers et réglementaires :

- **Bâle 2**
 - Institutions bancaires : obligation d'allouer des réserves en fonds propres pour couvrir les risques opérationnels attachés à leurs engagements (8% des montants)
- • **SOX** (Sarbanes Oxley Act) :
 - les dirigeants d'entreprises de pouvoir produire des informations financières et comptables fiables, transparentes et secourues (**auditables**)
 - Responsabilité civile et pénale du chef d'entreprise
- **Législations sectorielles** (seuils sites classés / Traçabilité médicale, alimentaire, ... /Auditabilité / ...)
- **Assurance** (rester assurable et indemnisable, durcissement du marché)
- **Un contexte concurrentiel difficile :**
 - Exposition médiatique
 - Des engagements vis- à- vis des tiers à respecter : clients, partenaires, investisseurs, ..

- **Contraintes métiers et réglementaires**
 - **Bâle 2 / Institutions bancaires : Obligation d'allouer des réserves en fonds propres pour couvrir les risques opérationnels attachés à leurs engagements. (8% des montants)**

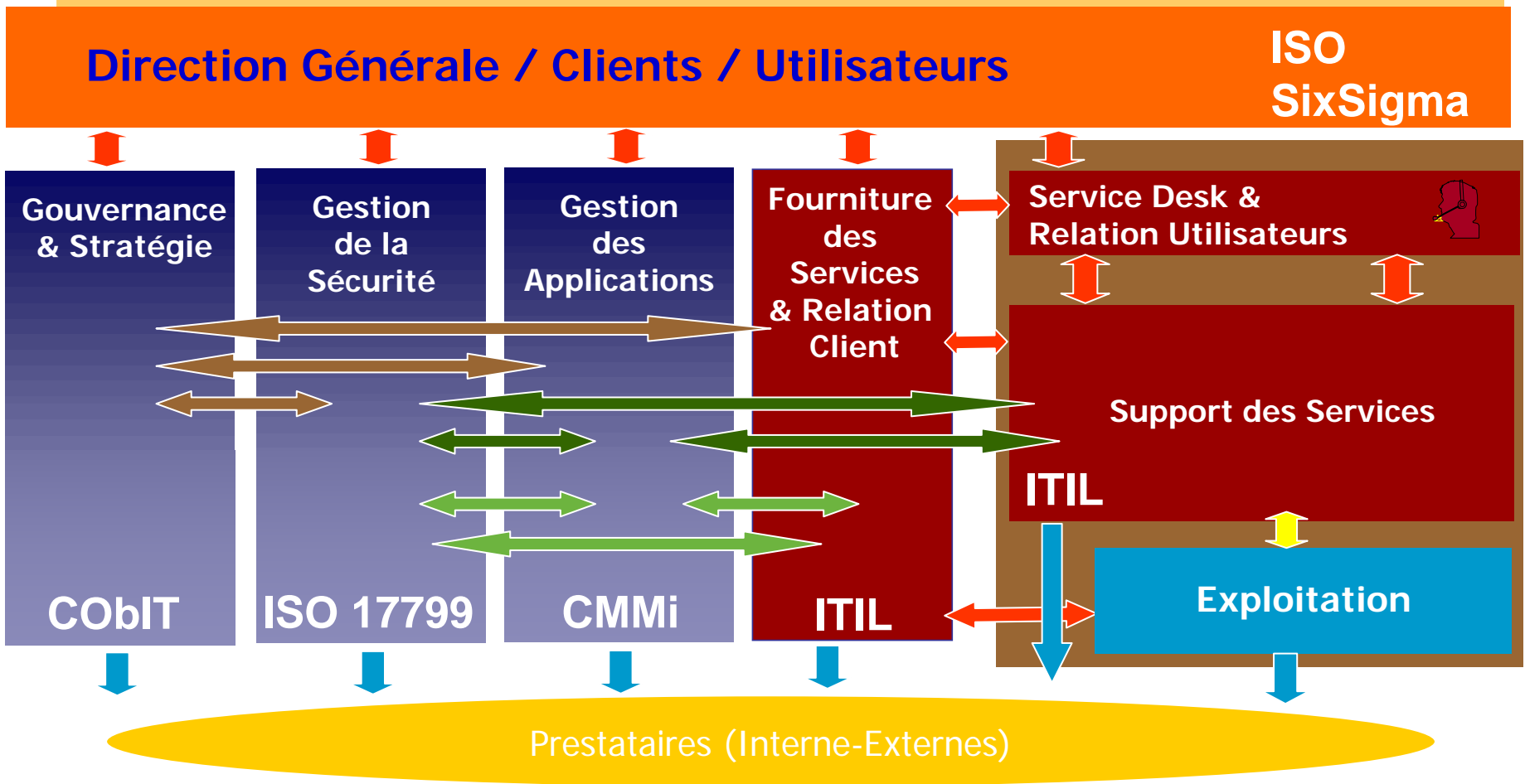


- le ratio de solvabilité



20% du ratio de 8%

- **SOX (USA: Sarbannes Oxley act) Informations financières et comptables fiables, transparentes, secourues et auditable ..**
- **Responsabilités Civile et pénale du chef d'entreprise**
- **Durcissement du marché de l'assurance**
- **Contexte concurrentiel difficile, business24/7, ...**



-  Stratégique
-  Tactique
-  Opérationnel

CobiT (Control Objectives for Business & Related Technology),
 Capability Maturity Model Integration® (**CMMI**).

Niveau	description
Niveau 0 - Incomplet	Les objectifs associés à ce secteur-clé ne sont pas remplis.
Niveau 1 - Réalisé	Les objectifs sont atteints, mais cette réussite repose essentiellement sur les individus.
Niveau 2 - Géré	traduit la mise en oeuvre effective de pratiques de base au niveau des projets mais sans harmonisation au niveau de l'organisation
Niveau 3 - Défini	traduit le déploiement harmonisé de pratiques définies au niveau organisation
Niveau 4 - Maîtrisé	traduit une gestion quantitative des processus, basée sur des analyses statistiques (les performances de l'organisation sont prévisibles).
Niveau 5 - En optimisation	traduit la maturité de l'organisation où veille technologique et amélioration continue concourent à l'excellence du processus.

Chiffres de la profession

Passage niveau 2 : 2 ans +
 Passage niveau 3 : 18 mois
 Passage niveau 5 : 2 ans –
 Dépense : 1500 US\$ / an / pers
 2 à 5 % du budget d'une organisation

Moyennes de la profession

Gains de productivité : 35 %
 Gains / détection défauts : 22 %
 Réduction « Time to Market » : 19 %
 Réduction des défauts post installation : 39 %
 ROI : 5 en 2 à 5 ans

- 4 domaines et 34 processus
- Chaque processus comprend
- une description, les entrées/sorties et les liens

OUTPUTS	to			
Risk assessment	PO1	ME3	DS5	DS12
Risk reporting	ME3			
IT-related risk management guidelines	PO6			
IT-related risk remedial action plans	PO4	AI6		

from	INPUTS
PO1	Strategic and tactical IT plans Service portfolio
DS5	Security threats
PO10	Project risk management plan
PO9	Contingency test results
ME1	Historical risk trends and events
DS2	Supplier risk

Exemple : PO9 Assess and manage IT risks

Activities	CEO	CFO	Business Executive	Senior Business Management	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance Audit Security and Risk	Configuration Manager
Develop configuration management planning procedures				C	A	C	I	C		C	R
Collect initial configuration information and establish baselines					C	C	C			I	A/R
Verify and audit configuration information (includes detection of unauthorised software)		I			A			I		I	A/R
Update configuration repository					R	R	R			I	A/R

Internal Control Example Segregation of Duties

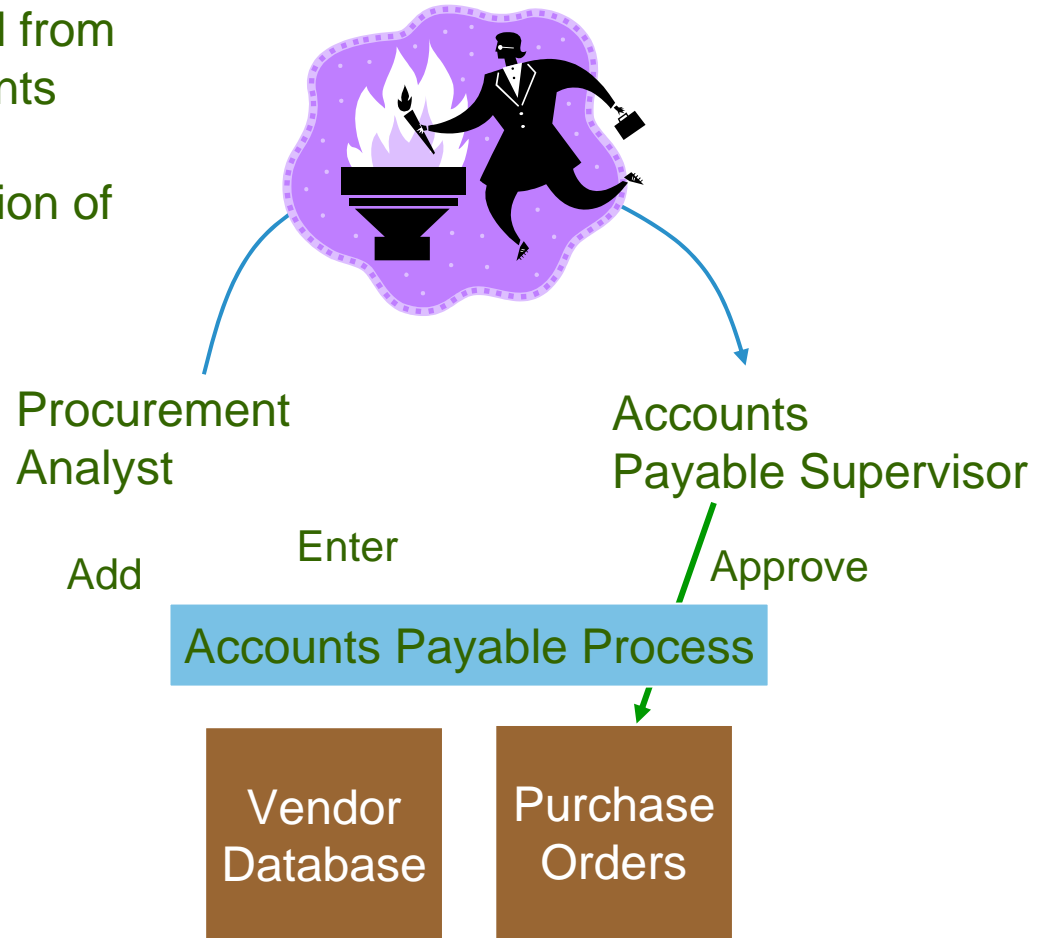
Scenario – A user is promoted from Procurement Analyst to Accounts Payable (AP) Supervisor

Control Objective – Segregation of duties between initiating and authorizing transactions

Controls needed –

- User Access

If the AP supervisor's access privileges are not updated upon promotion, they could be able to both initiate and approve payments



Copie de Mapping Cobit - ITIL - BS7799				
	A	B	C	D
133	8.3.1	Policy on the use of cryptographic controls	To maximise benefits and minimise the risks of using cryptographic techniques and to avoid inappropriate or incorrect use of cryptographic techniques.	To maximise benefits and minimise the risks of using cryptographic techniques and to avoid inappropriate or incorrect use of cryptographic techniques.
134	8.3.2	Encryption	To protect the confidentiality of business-critical information.	To protect the confidentiality of business-critical information.
135	8.3.3	Digital signatures	To protect the authenticity and integrity of electronic documents.	To protect the authenticity and integrity of electronic documents.
136	8.3.4	Non-repudiation services	To resolve disputes about the occurrence or non-occurrence of an event.	To resolve disputes about the occurrence or non-occurrence of an event.
137	8.3.5	Key management	To ensure the effective use of cryptographic techniques.	To ensure the effective use of cryptographic techniques.
138	8.4	Security of application system files	To ensure that IT projects and support files are conducted in a secure manner.	To ensure that IT projects and support files are conducted in a secure manner.
139	8.4.1	Control of operational software	To minimise the risk of corruption of operational systems.	To minimise the risk of corruption of operational systems.
140	8.4.2	Protection of system test data	Test data shall be protected and controlled.	Test data shall be protected and controlled.
141	8.5	Security in development and support process	To maintain the security of application system software and data	To maintain the security of application system software and data
142	8.5.1	Change control procedures	To minimise the risk of corruption of information systems.	To minimise the risk of corruption of information systems.
143	8.5.2	Technical review of operating system changes	To ensure that there is no adverse impact on operation or security.	To ensure that there is no adverse impact on operation or security.
144	8.5.3	Restrictions on changes to software packages	To restrict modifications to software packages.	To restrict modifications to software packages.
145	8.5.4	Covert channels and Trojan code	To minimise vulnerability to the introduction and retention of Trojan code.	To minimise vulnerability to the introduction and retention of Trojan code.
146	8.5.5	Outsourced software development	To mitigate the inherent risks in outsourced software development.	To mitigate the inherent risks in outsourced software development.
147	9	Business continuity management	To counteract interruption to business activities and protect critical business processes from the effect of disasters.	To counteract interruption to business activities and protect critical business processes from the effect of disasters.
148	9.1	Aspects of business continuity management	To have plans available to counteract interruptions to business activities.	To have plans available to counteract interruptions to business activities.
149	9.1.1	Business continuity management process	To establish a managed process for developing and maintaining business continuity plans across the organization.	To establish a managed process for developing and maintaining business continuity plans across the organization.
150	9.1.2	Business continuity and impact analysis	To determine the likely impact of expected interruptions in terms of damage and recovery.	To determine the likely impact of expected interruptions in terms of damage and recovery.
151	9.1.3	Writing and implementing continuity plans	To ensure that business operations are restored within the required recovery period.	To ensure that business operations are restored within the required recovery period.
152	9.1.4	Business continuity planning framework	To ensure that all plans are consistent, and to identify priorities for testing and maintenance.	To ensure that all plans are consistent, and to identify priorities for testing and maintenance.
153	9.1.5	Testing maintaining and re-assessing business continuity plans	Controls are in place to ensure that the continuity plan will work in real life:	Controls are in place to ensure that the continuity plan will work in real life:
154	10	Compliance	1. Table-top testing of various scenario's. 2. Simulations. 3. Technical recovery testing. 4. Testing recovery at an alternative site. 5. Test of supplier facilities and services (ensuring that externally provided services meet with requirements) 6. Complete rehearsals. 7. Situations that might necessitate updating of plans are integrated into continuity reviews. It includes changes in: 7.1 Personnel. 7.2 Addresses and telephone numbers. 7.3 Business strategy. 7.4 Location, facilities and resources. 7.5 Legislation. 7.6 Contractors, suppliers and key customers. 7.7 Processes or new/withdrawn ones. 7.8 Risks	1. Table-top testing of various scenario's. 2. Simulations. 3. Technical recovery testing. 4. Testing recovery at an alternative site. 5. Test of supplier facilities and services (ensuring that externally provided services meet with requirements) 6. Complete rehearsals. 7. Situations that might necessitate updating of plans are integrated into continuity reviews. It includes changes in: 7.1 Personnel. 7.2 Addresses and telephone numbers. 7.3 Business strategy. 7.4 Location, facilities and resources. 7.5 Legislation. 7.6 Contractors, suppliers and key customers. 7.7 Processes or new/withdrawn ones. 7.8 Risks
155	10.1	Compliance with legal requirements	To ensure compliance with legal requirements.	To ensure compliance with legal requirements.
156	10.1.1	Identification of applicable legislation	To ensure that all applicable legislation is identified.	To ensure that all applicable legislation is identified.
157	10.1.2	Intellectual property rights	To ensure that intellectual property rights are protected.	To ensure that intellectual property rights are protected.
158	10.1.3	Safeguarding organizational records	To ensure that organizational records are protected from loss, destruction and falsification.	To ensure that organizational records are protected from loss, destruction and falsification.
159	10.1.4	Data protection and privacy of personal information	To ensure that personal information is protected from dissemination of personal information.	To ensure that personal information is protected from dissemination of personal information.
160	10.1.5	Prevention of misuse of information processing facilities	To ensure that information processing facilities are not misused.	To ensure that information processing facilities are not misused.
161	10.1.6	Regulation of Cryptographic controls	To ensure that cryptographic controls are regulated.	To ensure that cryptographic controls are regulated.
162	10.1.7	Collection of evidence	To ensure that evidence is collected.	To ensure that evidence is collected.
163	10.2	Review of security policy and technical compliance.	To ensure that security policies and standards are reviewed.	To ensure that security policies and standards are reviewed.
164	10.2.1	Compliance with the security policy	To ensure compliance with security policies.	To ensure compliance with security policies.

ISO/IEC Standard	Description
27000	Vocabulary and definitions
27001	ISMS (BS7799-2)
27002	Code of Practice (ISO17799:2005)
27003	Implementation Guidance
27004	Metrics and Measurement
27005	Risk Management (BS 7799-3/ISO 13335)



Telindus Arche

Jean Marc CHARTRES



Ne doit pas exclure bon sens et compétence

Pour Chris Argyris (Apprentissage Organisationnel 1970),

« nous nous emprisonnons dans des **routines défensives**. Elles protègent nos modèles mentaux de la moindre critique et débouchent sur un talent d'incompétence. »