

Les conséquences de Bâle II pour la sécurité informatique



PLAN GENERAL

PLAN

DO

CHECK

ACT

- Introduction :
- Présentation de l'ISO 17799
- Analyse de risque opérationnel
- Organisation de la sécurité
- Recommandations techniques
- Suivi de projet
- Dispositifs de continuité
- Indicateurs de suivi
- Gestion des incidents majeurs
- Présentation ITIL
- Références
- Mise en œuvre
- Conclusions



2001

Le comité de Bâle demande aux banques de se prémunir face aux risques dits opérationnels en 2004, notamment en ce qui concerne le : « **risque de pertes directes ou indirectes d'une inadéquation ou d'une défaillance attribuable à des procédures, personnes, systèmes internes ou à des évènements extérieurs** »

BNP-PARIBAS décide de se doter des outils de mise en conformité, de ses pôles et filiales, afin de lutter contre le risque de perte d'image.

2002

conséquences immédiates sur la politique sécurité ARVAL :


- ◆ mise en œuvre d'une méthode d'analyse et de suivi du risque opérationnel dans les projets :
l'ensemble des projets de la DSI fait l'objet d'une analyse de risque ainsi que la rédaction de recommandations sécurité pour l'infrastructure, le développement, la production et le respect des normes et standards internes.
- ◆ remontée d'informations sur les incidents majeurs et leur qualification technique et financière
- ◆ mise en œuvre des processus ITIL : Incident Management, problem Management et prise en compte de la continuité de manière globale.

ARVAL anticipe la notion de risque opérationnel en l'intégrant dès 2002..



- Un ensemble de contrôles basés sur les meilleures pratiques en sécurité des informations
- Complète les normes existantes en matière de SSI
 - ISO13335 (gestion de risques)
 - ISO15408 (évaluation)
 - FIPS140-2 (cryptographie)
 - etc.
- Standard international qui couvre tous les aspects de la sécurité informatique:
 - Équipements
 - Politiques de gestion
 - Ressources humaines
 - Aspects juridiques





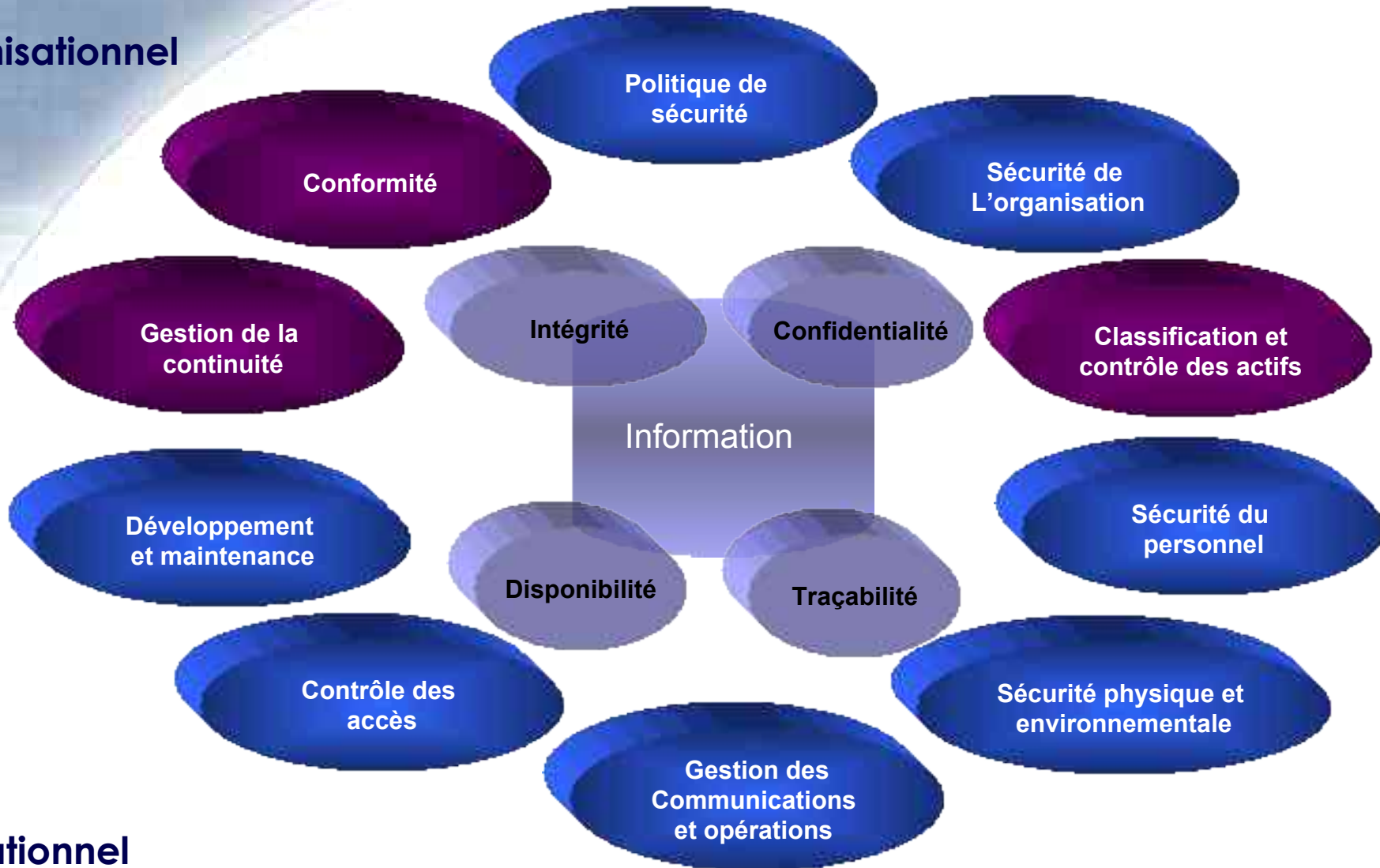
● ISO 17799 (partie 1) se veut un guide contenant des conseils et des recommandations permettant d'assurer la sécurité des informations d'une entreprise.

● BS 7799 (partie 2) propose des recommandations afin d'établir un cadre de gestion de la sécurité de l'information efficace.

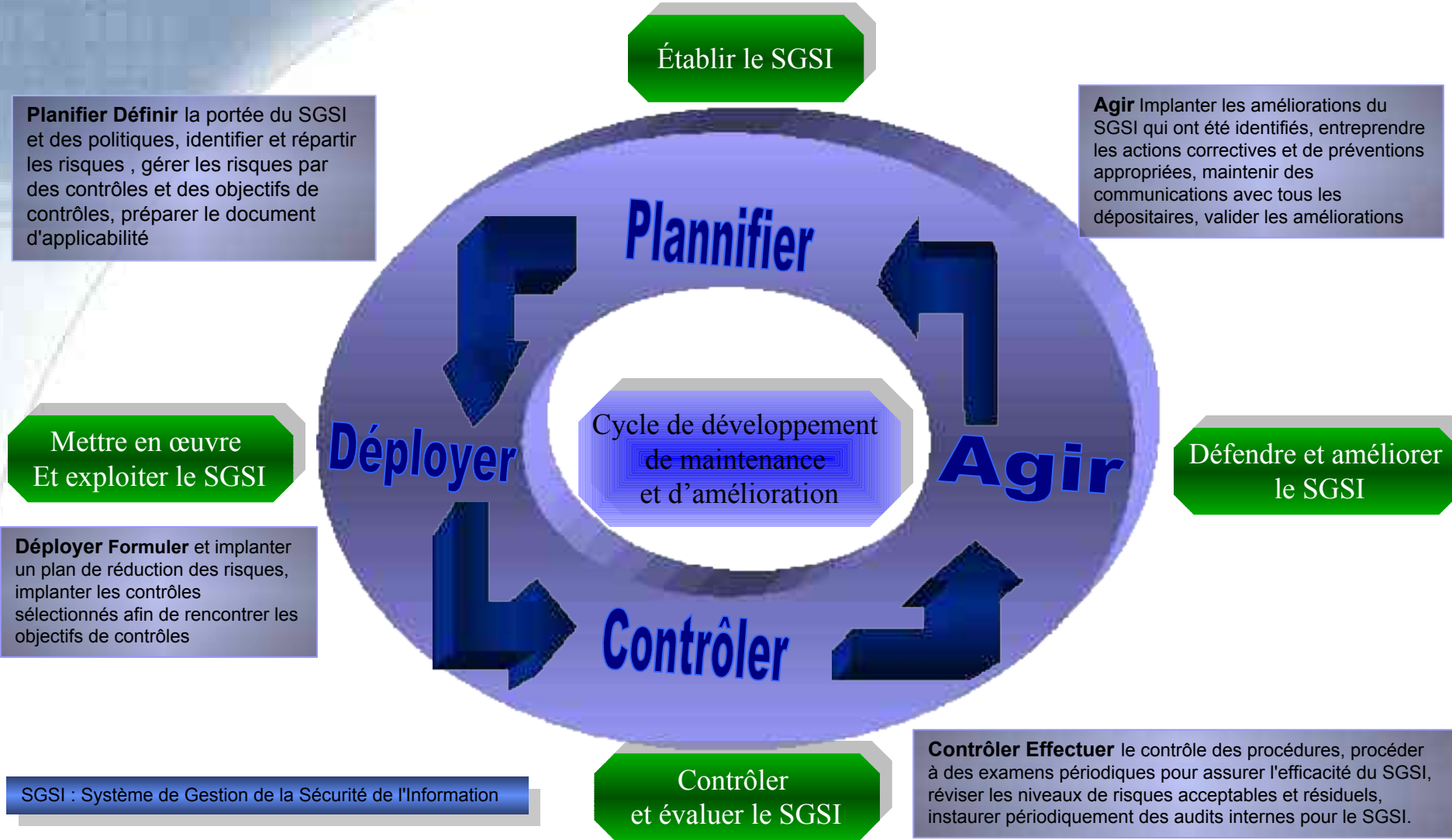
BS 7799-2 permet d'établir un système de gestion de sécurité de l'information (SGSI).

- 1^{ère} certification française en MAI 2005 ISO 27001.
- Une démarche d'audit peut être appuyée:
 - Vérification interne
 - Vérification externe (lettre d'opinion)
 - Bureau de registraire du BSI (certification officielle)

Organisationnel



POLITIQUE SECURITE ET NORME ISO 17799



SGSI : Système de Gestion de la Sécurité de l'Information

DO

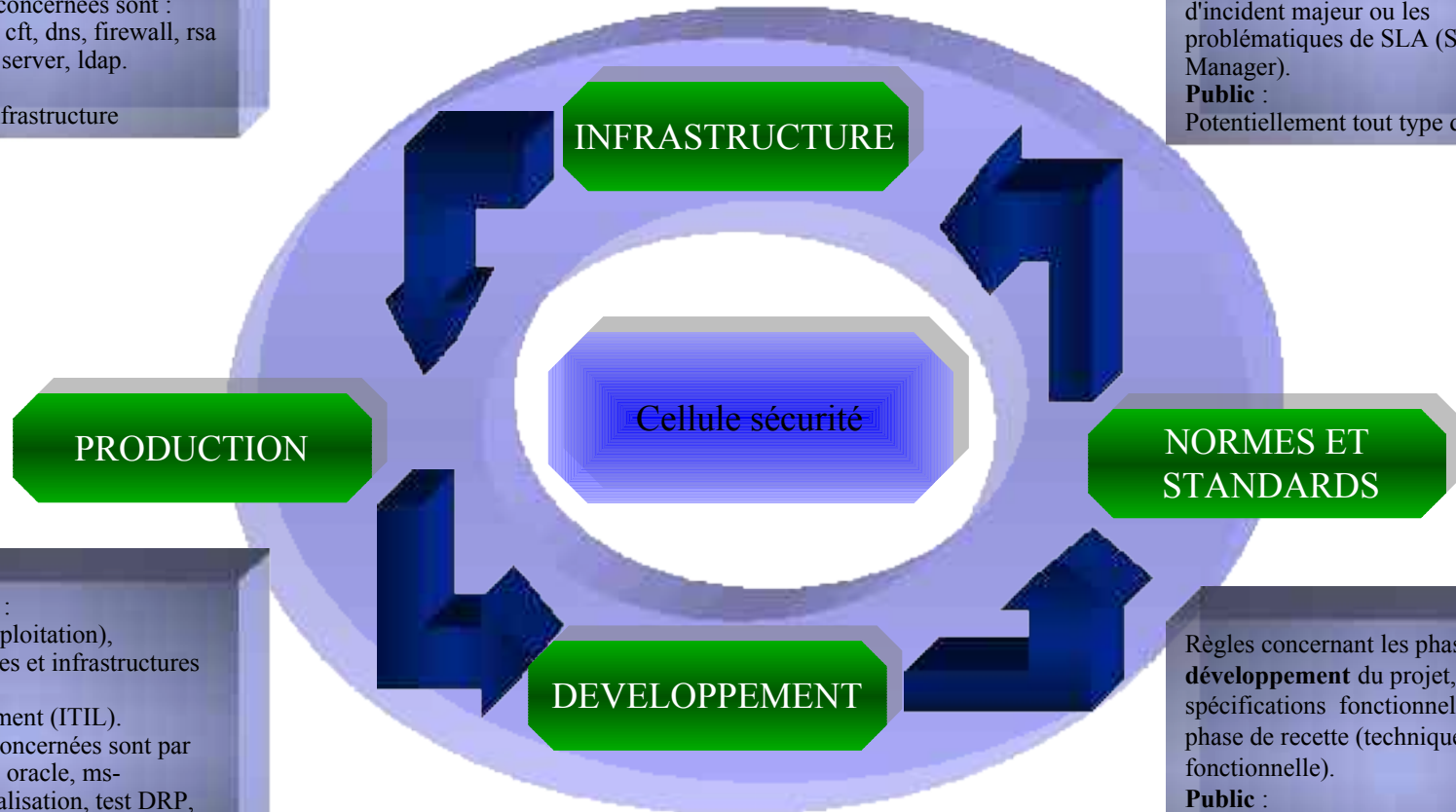
ANALYSE DE RISQUE OPERATIONNEL

			CONFIDENTIALITE	INTEGRITE	DISPONIBILITE	AUDITABILITE
RISQUES POTENTIELS	↑ ↓ ↘ ↗ ↖ ↗		Divulgateion ou perte	Modification erronée ou illicite	indisponibilité dans les délais requis pour l'exécution d'une opération + Délaï Maximum d'Interruption Autorisée + Perte de Données Tolérée	Perte du traçage d'information, disparition des preuves
Sans conséquences sur l'activité. Sans conséquence sur l'image Arval Perte financière < 10 000 €	(NON SENSIBLE	NON SENSIBLE	NON SENSIBLE	PAS DE PREUVE
Atteinte à l' activité ayant un caractère faible Risque d' image ayant un caractère faible Risque de ressource humaine faible Risque juridique faible Perte financière < 50 000 €	,		CONFIDENTIEL ARVAL	PROTEGE ARVAL	PROTEGE ARVAL Action corrective inférieure à 4 jours Document de reprise obligatoire	PREUVE ARVAL <= 1 MOIS
Atteinte à l' activité à caractère moyen Risque d' image ayant un caractère moyen Risque de ressource humaine moyen Risque juridique moyen Perte financière < 100 000 €	;		HAUTEMENT CONFIDENTIEL ARVAL	STRATEGIQUE ARVAL	STRATEGIQUE ARVAL Action corrective inférieure à 2 jours - Document de reprise - 1 test DRP annuel	PREUVE ARVAL <=12 MOIS
Atteinte à l' activité ayant un caractère fort Risque d' image ayant un caractère fort Risque de ressource humaine fort Risque juridique fort Perte financière > à 100 000 €	;		SECRET ARVAL	VITAL ARVAL	VITAL ARVAL ₁ Action corrective inférieure à ½ journée - Document de reprise - Dispositif d'alerte défini - 1 test BCP annuel - SLA signé entre la DSI et le métier	PREUVE PERMANENTE ARVAL

ORGANISATION DE LA SECURITE DANS LES PROJETS

Règles concernant les départements **Infrastructure**, réseau, telecom, Servers & Desktops ,
Les technologies concernées sont : serveurs, masters, cft, dns, firewall, rsa securID, terminal server, ldap.
Public :
Chefs de projet Infrastructure

Règles concernant tout **processus transverse** à l'ensemble de la DSI (direction des systèmes d'information) comme par exemples les remontées d'incident majeur ou les problématiques de SLA (Service level Manager).
Public :
Potentiellement tout type d'acte



Règles concernant : les **opérations** (exploitation), les bases de données et infrastructures applicatives, le change management (ITIL).
Les technologies concernées sont par exemples : sybase, oracle, ms-sql, backup, externalisation, test DRP, exploitation, batchs,
Public :
Chefs de projet Production

Règles concernant les phases de **développement** du projet, des spécifications fonctionnelles jusqu'à la phase de recette (technique & fonctionnelle).
Public :
Chefs de projet Développement, et par extension à tout développeur interne ou externe

	CONFIDENTIALITE	INTEGRITE	DISPONIBILITE		AUDITABILITE
NIVEAU	Divulgarion ou perte	Modification erronée ou illicite	Indisponibilité dans les délais requis pour l'exécution d'une opération		Perte du traçage d'information, disparition des preuves
			Mesures	Fréquence des back-up	
0	<ul style="list-style-type: none"> ✦ Identification des biens manipulés par le projet (<i>biens du système cible et biens propres au projet</i>) et classification de ces biens (<i>ISO Introduction et § 5</i>) ✦ Identification nominative des responsabilités propres au projet (<i>Chef de Projet MOA, Chef de projet MOE, développeurs, exploitant, responsable infrastructure, ...</i>) <i>ISO § 4.1</i> ✦ Engagements de sécurité pour tout intervenant (<i>vérification des références lors du recrutement, contrat de travail avec engagement de confidentialité et de respect des règles en vigueur et engagements systématique pour les sous traitants</i>) : <i>ISO § 6</i> ✦ Exigences contractuelles standard vis-à-vis des tiers intervenant sur le projet (<i>ISO § 4.2</i>) ✦ Respect des procédures internes http://intra.arval.fr/moe/securete/themes/fr/procedures/index.htm ✦ Demande de dérogation formelle et préalable auprès de l'équipe sécurité pour tout non respect des exigences ✦ Intégration de fiches de sécurité dans le cahier de recette ✦ Sécurisation de l'ensemble des composants du système d'information conformément aux règles internes 				
D E V E L O P P E M E N T	<ul style="list-style-type: none"> ✦ Formation des développeurs aux techniques de sécurité / sensibilisation sécurité des intervenants projet (<i>ISO § 6.2</i>) ✦ Veille sur les failles / nouvelles technologies ou fonctions de sécurité (<i>ISO § 6.3.2. ...</i>) ✦ Utilisation d'un gestionnaire de versions sécurisé ✦ Utilisation d'un outil de contrôle automatique du code (fxcop par exemple pour les technologies) ✦ Documentation du code source ✦ Les progiciels ne doivent pas faire l'objet de modifications directes ; Elles doivent être réalisées par l'éditeur et rentrer dans le cadre du support <i>ISO §10.5.3</i> 				
	Stockage des paramètres de connexion en local interdit	Définition de chaque format de données utilisées. Mise en œuvre des contrôles correspondants pour se protéger des différents types d'injection de code (Cross Site Scripting, SQL injection & Buffer overflow) Validation des fichiers uploadés (taille, virus, type)	Sauvegarde complète régulière + sortie des supports du site	Sauvegardes quotidiennes Sortie hebdo des supports	Chaque accès au code en modification doit être tracé (<i>cf. gestionnaire de versions</i>). Les développeurs doivent s'authentifier de manière nominative. Information des intéressés sur les données conservées (<i>exigences CNIL</i>)
P R O D U C T I O N	<ul style="list-style-type: none"> ✦ Respect des procédures internes. ✦ Protection physique des serveurs conformément aux règles internes (y compris en phase projet (<i>niveau à déterminer</i>) <i>ISO § 7</i>) 				
	X	X	1 sauvegarde interne des sources après mise en production de chaque nouvelle version. Procédure d'arrêt « propre ». Tests réguliers des supports de sauvegarde (<i>ISO § 8.4</i>) Protection physique des supports amovibles (<i>ISO § 8.6</i>) et de sauvegarde (<i>ISO § 8.4</i>)	Sources : 1 fois, après la MEP	Conservation des sources : +∞

CONFIDENTIALITE		INTEGRITE	DISPONIBILITE		AUDITABILITE
Divulgarion ou perte		Modification erronée ou illicite	Indisponibilité dans les délais requis pour l'exécution d'une opération		Perte du traçage d'information, disparition des preuves
			Mesures	Fréquence des back-up	
I N F R A S T R U C T U R E	<ul style="list-style-type: none"> ✦ Mutualisation sur un même serveur d'applications ou de données de mêmes niveaux de classification ✦ Seuls les services indispensables doivent être actifs sur les serveurs 				
	Cloisonnement réseau permettant notamment de joindre le serveur d'hébergement de l'application uniquement sur les ports requis par cette dernière.		Mise en œuvre du service anti-virus sur l'infrastructure cible (procédures d'acquisition de codes, mise en œuvre et maintien en conditions opérationnelles d'un anti-virus, scan régulier, ...) ISO § 8.3.1.	X	Synchronisation des horloges de l'ensemble des équipements ISO §9.7.3
P R O C E S S	<ul style="list-style-type: none"> ✦ Les procédures opérationnelles projet doivent être formalisées (<i>accès aux informations, réaction aux erreurs ou interrogations, ...</i>) en incluant la procédure de gestion des incidents de sécurité ISO § 8.1.3 ✦ L'analyse des besoins et les spécifications doivent inclure des chapitres dédiés à la sécurité. ISO §10.1.1 ✦ Une analyse d'impact du projet sur le reste du système d'information doit être réalisée ISO §10.5.1 ✦ Les procédures de recette doivent notamment comprendre les éléments suivants : contrôle des exigences de performance, procédure de retour arrière et plan d'urgence, cahier de tests formel et complet, test de chaque fonction de sécurité, les preuves que le nouveau système n'affectera pas les systèmes en place (non régression) et la formation des acteurs impliqués. ISO § 8.2.2. • Aucune mise en production n'est réalisée sans validation de la recette ni épuration dans le code des parties utilisées lors des développements ISO §12.4.1 • Les procédures de surveillance des événements de sécurité doivent être formalisées. ISO § 9.7.2 • Chaque nouveau projet doit intégrer le plan de continuité défini par l'entreprise. ISO §11.1 • Un contrôle doit être réalisé pour s'assurer que le projet n'enfreigne aucune disposition légale ISO §12.1.1 • Les droits à la propriété intellectuelle concernant tous les composants utilisés doit être respectée. ISO §12.1.2 • Les utilisateurs du système d'information doivent être informés de leurs droits et de leurs devoirs vis-à-vis du système d'information ISO §12.1.5 • Tout audit du système doit se faire dans un cadre précis afin de : <ul style="list-style-type: none"> - Minimiser les impacts sur le travail au sein de la structure - Ne pas nuire à la sécurité de la structure ISO §12.3 				
	Respect des procédures internes	Stockage des programmes, logiciels, documentations dans la DSL (Definitivre Software Library) (notion ITIL)	X	X	X

NIVEAU 3	CONFIDENTIALITE	INTEGRITE	DISPONIBILITE		AUDITABILITE
	Divulgarion ou perte	Modification erronée ou illicite	Indisponibilité dans les délais requis pour l'exécution d'une opération		Perte du traçage d'information, disparition des preuves
			Mesures	Fréquence des back-up	
DEVELOPP-EMENT	Niveau 2	Niveau 2 Contrôle : Audit applicatif	Niveau 1	X	Niveau 0
PRODUCTION EXPLOITATION	Destruction physique irréversible de tout support de données ayant contenu des données classifiées N3 devenu inutile (ISO § 8.6.2.)				
INFRA-STRUCTURE	Limitation des accès par contrôle réseaux et physique.	Niveau 2 Surveillance 24 – 24 7-7	Shadowing + striping : RAID 1+ 0. Sauvegarde de type interne et externe. Onduleurs de type : IN-LINE.	Données Sauvegarde interne : snapshot toutes les 2h et sauvegarde totale quotidienne Sauvegarde externe : toutes les ½ journées. Sources Sauvegarde interne : toutes les 4h. Sauvegarde externe : toutes les ½ journées.	Niveau 2 + Centralisation et corrélation des logs et journaux d'évènements + Service d'alerte 24-24 7-7
PROCESS	<ul style="list-style-type: none"> 🛡️ Protection physique des supports (dossiers papier, sortie d'imprimante, PC portable) ISO §7.3 🛡️ Séparation des responsabilités au sein des projets sensibles (notamment <i>les spécifications, le développement et le contrôle pour les fonctions sensibles</i>) ISO § 8.1.4. 				
	Niveau 1 + Validation par un RSSI et direction générale de l'autorisation de diffusion d'une information de type3.	Niveau 2 + alerte de la direction générale par mail, SMS, et téléphone.	Niveau 2 Remonté d'incident en cas de problème par l'administrateur de l'application au RSSI, DSI, chef de service et direction générale par mail, SMS, et téléphone. Compte-rendu d'incident majeur	<ul style="list-style-type: none"> 🛡️ Action corrective inférieure à ½ journées 🛡️ Document de reprise 🛡️ SLA signé entre la DSI et le métier 🛡️ 1 test PCA annuel 	Conservation des traces : +∞ permanent

PHASES PROJET

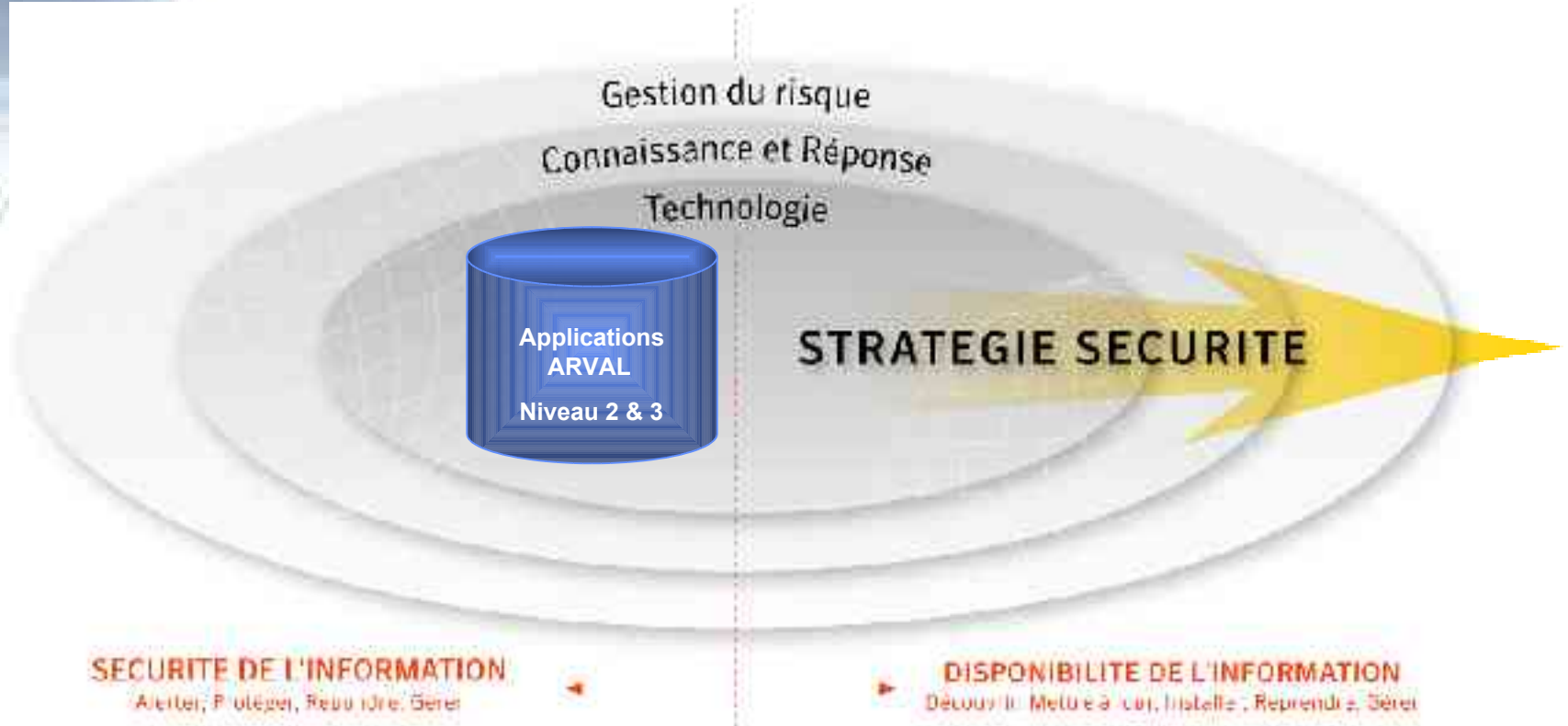
Plan

Do

Check

N°	Phase	Responsable avancement	Fin de la phase	Etape et livrable sécurité
1	Idée	Clients	Rédaction d'une première version du document de cadrage	
2	Structuration	Client principal	Signature du document de cadrage et validation CSI	Etape 1 : Classification des informations Livrable : Document de classification R-1-FR-SECU-F-Arval-Phh_classification_du_projet_MOAXXX
3	Etudes	Selon le type d'étude	Selon de type d'étude	Etape 2 : Initialisation de la rédaction du contrat de service et de la procédure de reprise d'activité Etape 3 : Préconisations Développement I et process Livrable : R-1-FR-SECU-F-Arval-Phh_Classification_et_synthese_recommandations_sécurité_CODE PROJET
4	Conception	MOE	Signature des spécifications détaillées rédigées par la MOA	Etape 4 : Finalisation des recommandations sécurité Développement II, Préconisation sécurité pour l'Infrastructure et la Production Livrable : R-1-FR-SECU-F-Arval-Phh_Classification_et_synthese_recommandations_sécurité_CODE PROJET
5	Réalisation	MOE	Livraison des programmes dans l'environnement de recette par la MOE	
6	Récette fonctionnelle	Client principal	Signature du PV de recette	Valider la mise œuvre des recommandations sécurité
7	Mise en production	MOA + client principal	Levée des réserves par le client principal	Etape 5 : Signature SLA et procédure de reprise d'activité Livrables : - Contrat de service SLA signé par la DSI et les Directeurs métiers impactés - Procédure de reprise d'activité signée par le DSI, RSSI, Responsable I&P P-14-FR-SECU-E-Arval-Phh_Appli
8	Homologation	MOA + client principal	Signature du PV d'homologation et validation des charges réelles du projet	Etape 6 : Certificat de conformité Livrable : R-1-FR-SECU-F-Arval-Phh_certificat_conformite_projet_MOAXXX

DEVELOPPEMENT ET RISQUE OPERATIONNEL



Répondre au niveau de risque opérationnel

QUALIFICATION DES INCIDENTS MAJEURS

- P-4-F-Arval-Phh_Gestion_des_Incidents_Majeurs_v1
- R-4-F-Arval_Ph_h_Compte-rendu-incident-majeur-type_v8
- T-4-F-Arval_Ph_h_Tableau_de_bord_incidents_majeurs_v4

liée à l'information et déclenchée par :

- ⊙ DATE DE L'INCIDENT
- ⊙ DESCRIPTIF COURT DE L'INCIDENT
- ⊙ DESCRIPTIF DÉTAILLÉ DE L'INCIDENT
- ⊙ RISQUES
- ⊙ IDENTIFICATION DES CAUSES
- ⊙ ACTIONS ET SOLUTIONS
- ⊙ RÉCAPITULATIF DES ACTIONS À MENER
- ⊙ TOTAL DU TEMPS CORRECTIF ESTIMÉ EN JOUR
- ⊙ ESTIMATION DE LA PERTE POSSIBLE (DU MANQUE À GAGNER)
- ⊙ CONSIDÉRATIONS TECHNIQUES
- ⊙ CONCLUSIONS ET REMARQUES PARTICULIÈRES

- ✓ La direction du système d'information
- ✓ Les chefs de service,
- ✓ Le RSSI,
- ✓ Le contrôle général.



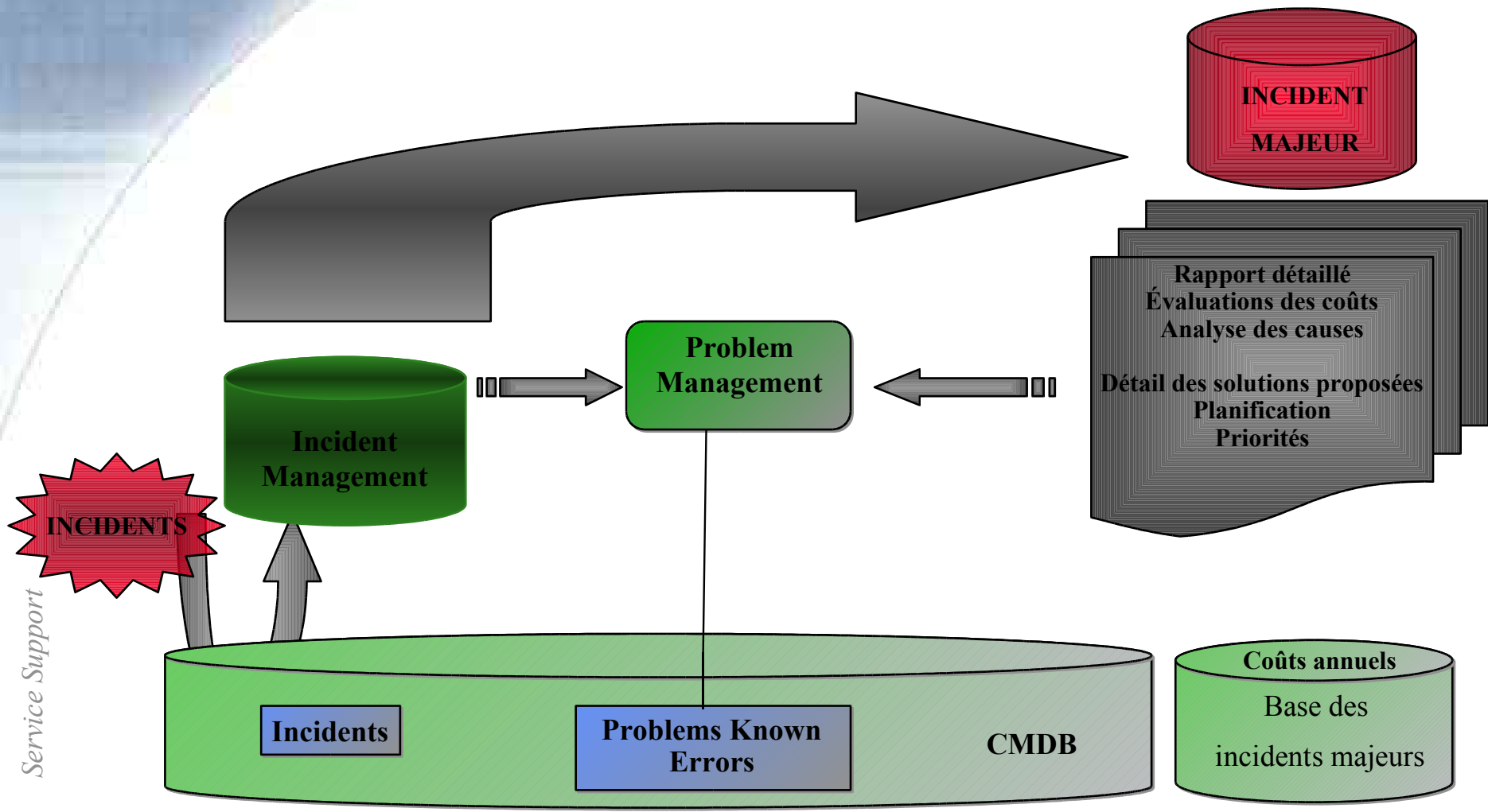
Objectifs :

- ✓ Ne pas reproduire
- ✓ Améliorer nos dispositifs
- ✓ Évaluer les pertes et provisionner

Destinataires:

- ✓ La direction du système d'information
- ✓ Le RSSI

PROVISION SUR INCIDENTS



Service Support

Information

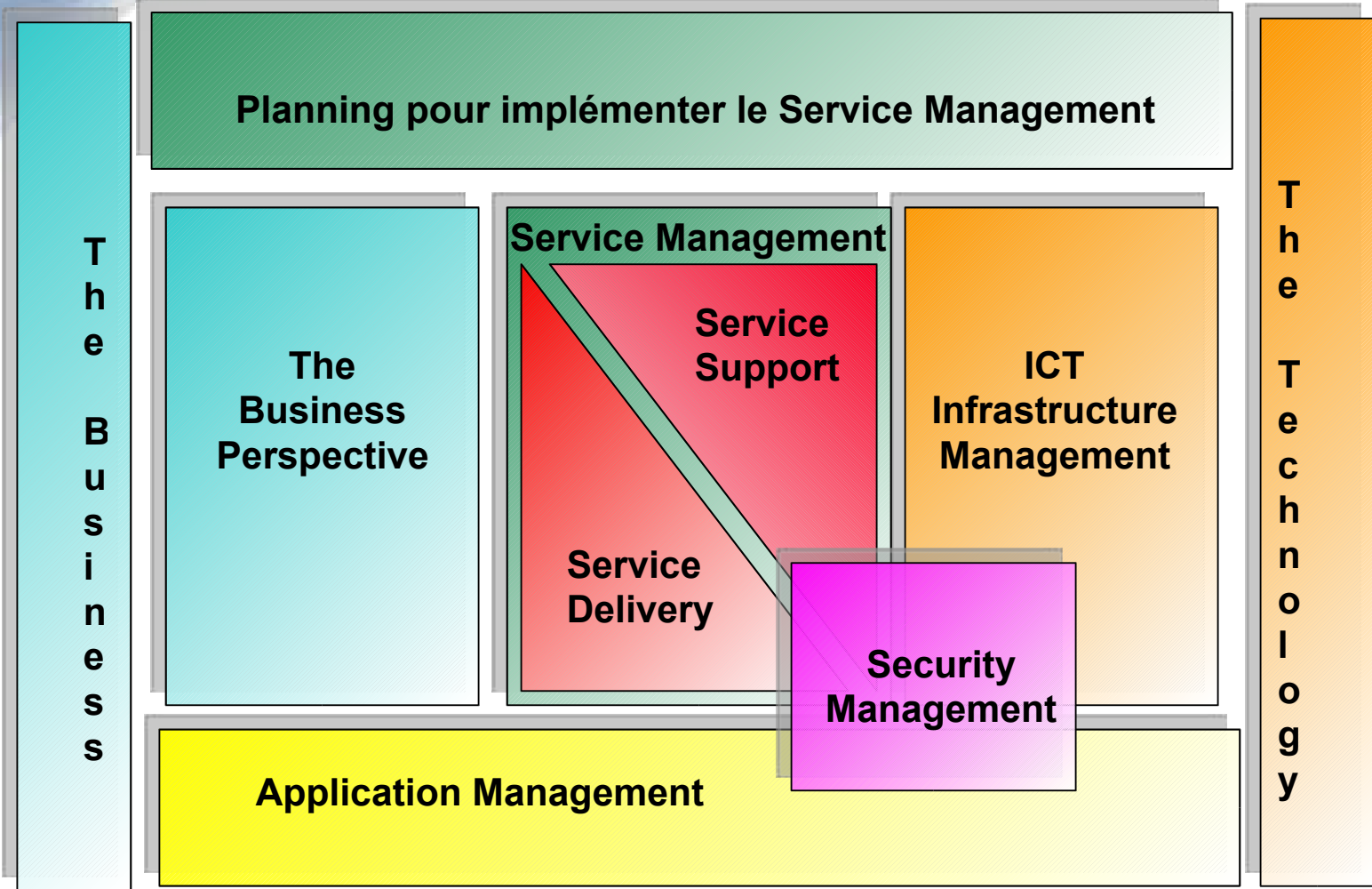
Technology

Infrastructure

Library

- **Un référencement des bonnes pratiques et une expérience concentrée pour faciliter la gestion de la qualité des services IT**
- **Non propriétaire**
- **Rédigée pour une qualité des standards tout en s'alignant sur ISO9001, BSI, EFQM**
- **Fondation pour le BS15000**

ENVIRONNEMENT ITIL



ITIL

- **Service Support**
 - Day to day operational support of IT services
- **Service Delivery**
 - Long term planning and improvement of IT service provision

Key Definitions

Customer: recipient of a service: usually the Customer management has responsibility for the ***funding*** of the service.

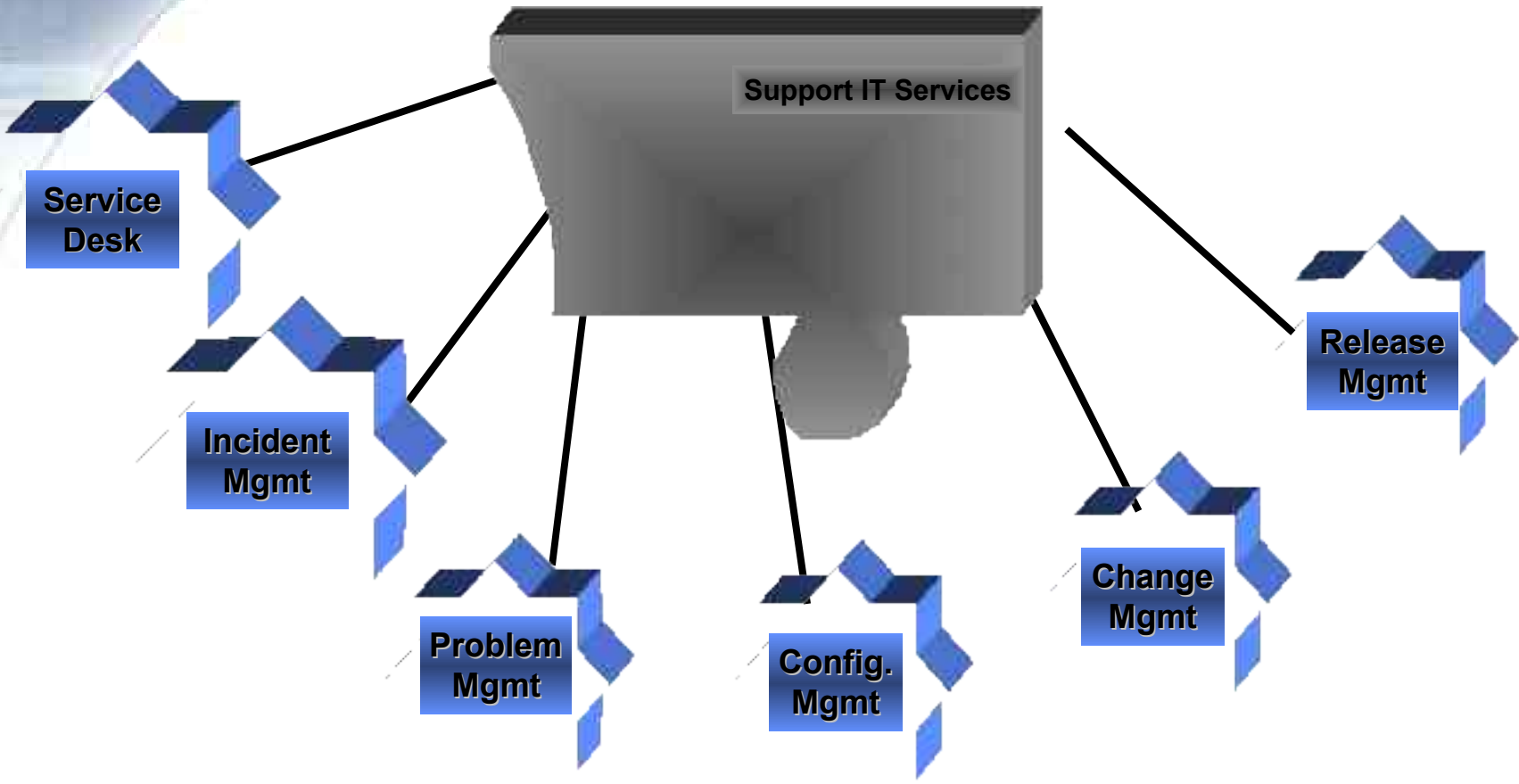
Provider: the unit responsible for the ***provision*** of IT service.

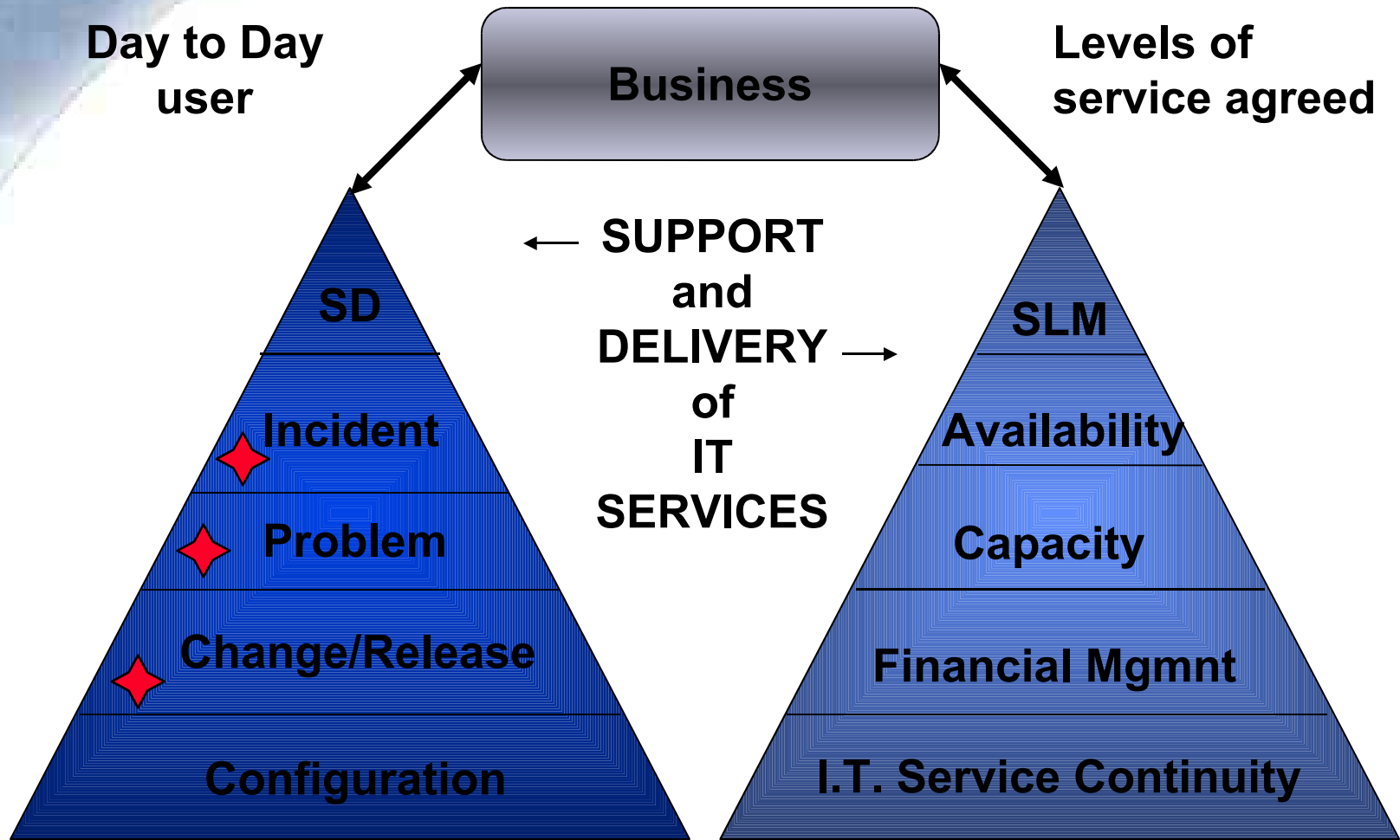
Supplier: a third party responsible for ***supplying*** or supporting underpinning elements of the IT service

User: the person ***using*** the service on a daily basis

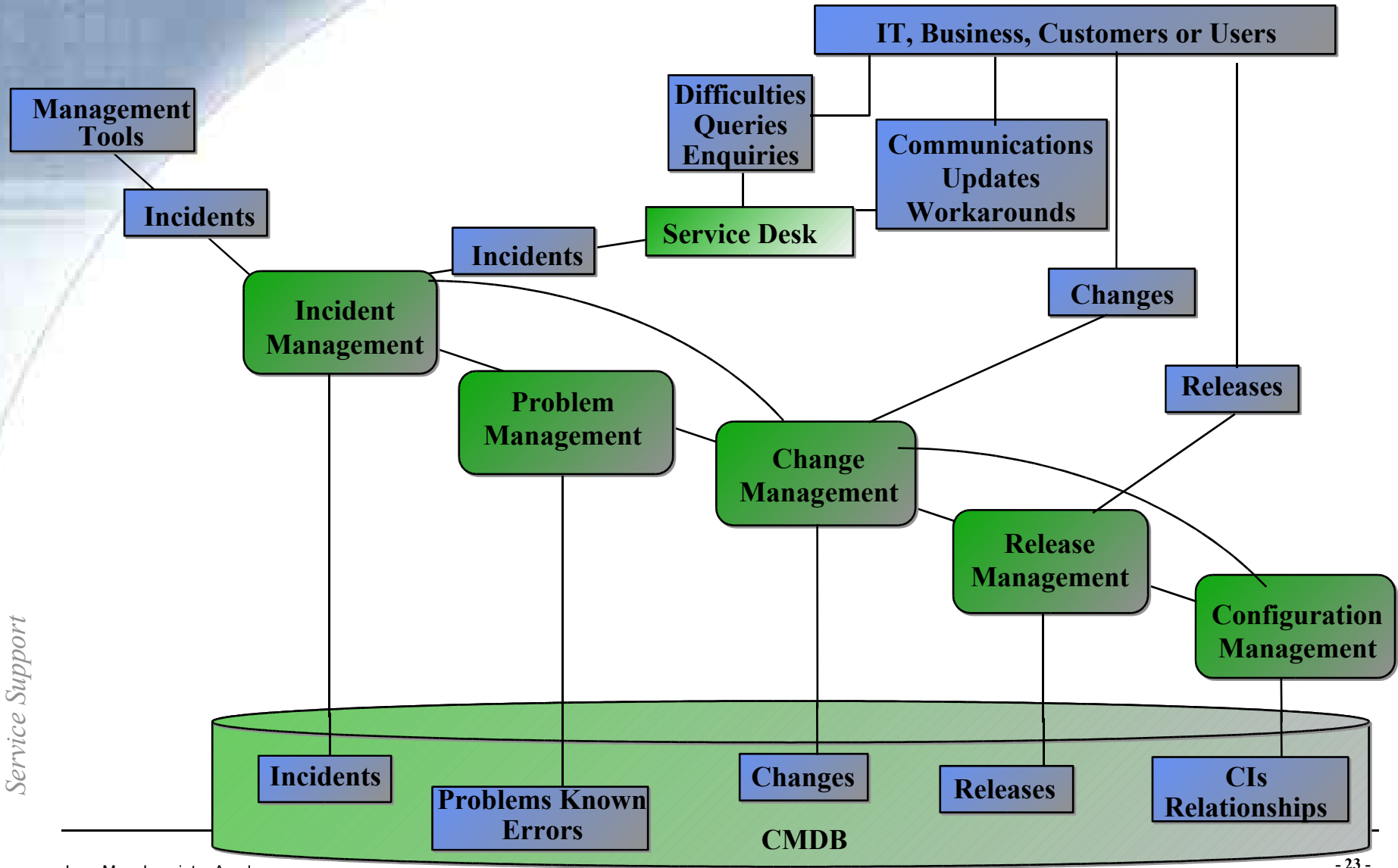
IT SERVICE SUPPORT

Service Support



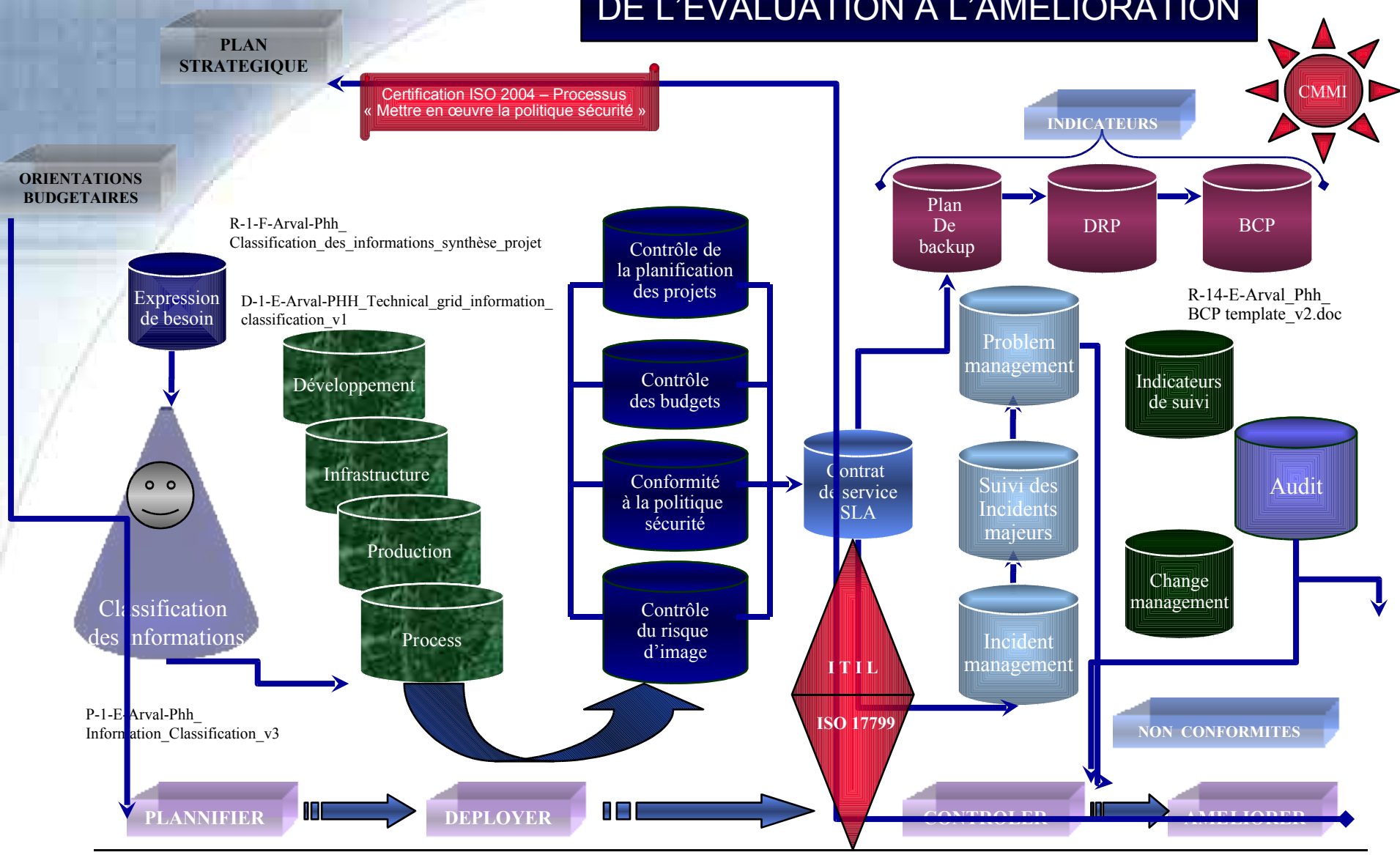


SERVICE SUPPORT PROCESS MODEL



Service Support

DE L'EVALUATION A L'AMELIORATION



CONCLUSIONS



- ◆ L'évaluation sur fond propre doit se définir à partir des éléments tangibles
- ◆ L'analyse de risque opérationnel doit concourir à mettre en place des solutions adaptées au niveau de problème.
- ◆ La continuité s'inscrit dans une démarche initiale de classification du risque opérationnel ayant pour vocation de « limiter les risques de défaillances »
- ◆ Elle doit limiter les risques de pertes directs en travaillant sur les axes de continuité et des systèmes de mesures (indicateurs).
- ◆ Elle peut être fédératrice des normes et méthodologies internes (exemple ITIL + ISO)
- ◆ Sa prise en compte dès le départ des projets permet, à terme, de simplifier les processus de suivi.
- ◆ Il y a nécessité de mettre en place un « Système de Management de la Sécurité des Informations » ou « SMSI pour :
 - Identifier correctement les besoins de sécurité
 - Transformer l'expression de besoins en recommandations
 - Développer la confiance dans la conformité et l'efficacité des mécanismes mis en œuvre
 - S'assurer que les risques résiduels sont tolérables
 - Regrouper tous ces aspects dans une approche intégrée

La continuité d'activité ne peut être perçue que de manière globale.
Elle débute dans les nouveaux projets avec une qualification des niveaux de continuité par l'analyse de risque opérationnel, elle accompagne le business et la production, et mesure régulièrement sa capacité de redémarrage

REFERENCES

- Documents BSI (www.bsi.org.uk/index.xhtml)
- *Information Security Management: An Introduction* (PD3000)
Fournit une vue d'ensemble du fonctionnement pour la certification accréditée et forme une préface utile aux autres guides.
- *Guide to BS7799 Risk Assessment and Risk Management* (PD3002)
Décrit les concepts sous-jacents à l'évaluation de risque de BS 7799, y compris la terminologie, le processus d'évaluation et la gestion de risque.
- *ISO/IEC Guidelines for the Management of IT Security* (GMITS)
- *Selecting BS7799 Controls* (PD3005)
Décrit le processus de sélection des commandes appropriées.



Jean-Marc Lecoïnt

Head of IT Security - Continental Europe
22 rue des 2 Gares
92564 Rueil Malmaison

Phone : + 33 (0) 1 57 69 68 42 - Fax : + 33 (0) 1 57 69 68 42
jean-marc.lecoïnt@arval.fr

Jmarc_lecoïnt@yahoo.fr

<http://www.arval.fr>

securite.SI@arvalphh.fr