L'AUDIT DES SYSTEMES D'INFORMATION

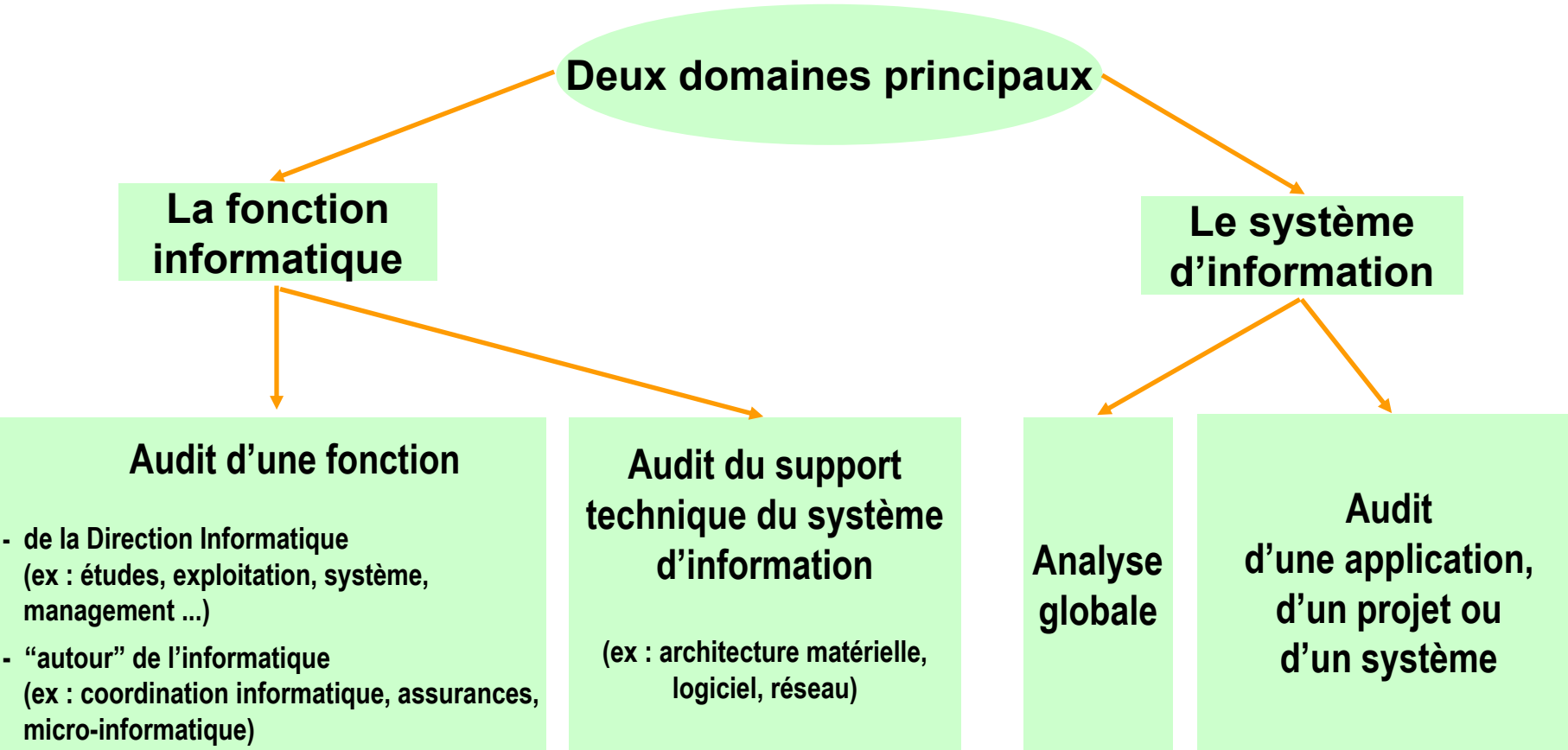
ESCI - Bourg en Bresse

(2005 – 2006)

- GENERALITES SUR L'AUDIT ➔
- AUDIT FONCTIONNEL OU D'APPLICATION ➔
- AUDIT DES FONCTIONS INFORMATIQUES ➔

Généralités sur l'Audit

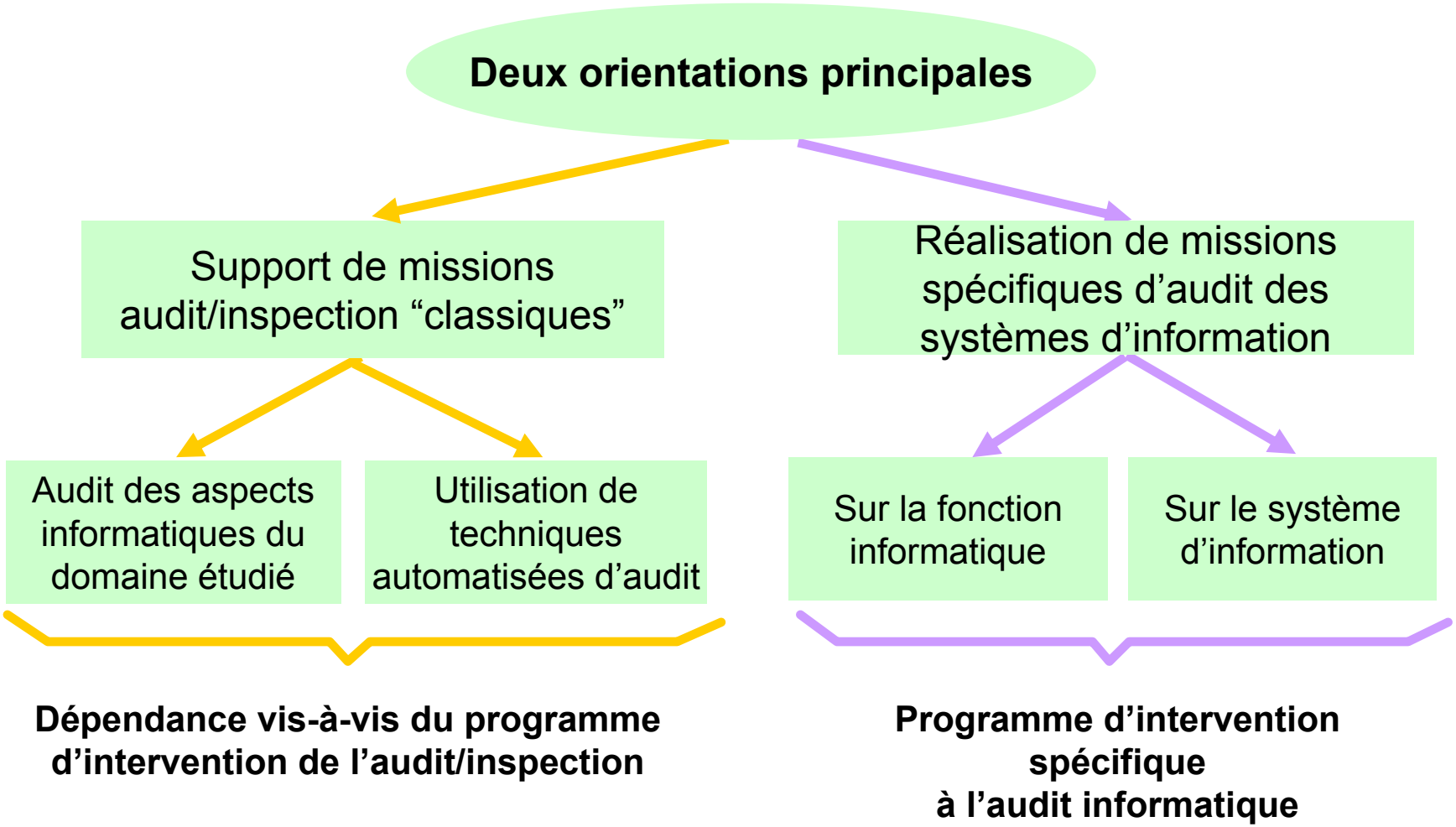
Qu'est-ce que l'audit des systèmes d'information ?



Typologie des travaux d'audit des systèmes d'information

- Les missions d'audit des systèmes d'information sont principalement caractérisées par :
  - Leur nature.
  - Les objectifs.
  - Le degré d'approfondissement des travaux
  - Leur caractère ponctuel ou permanent.

Qu'est-ce que l'audit des systèmes d'information ?



Qu'est-ce que l'audit des systèmes d'information ?

Deux catégories d'objectifs

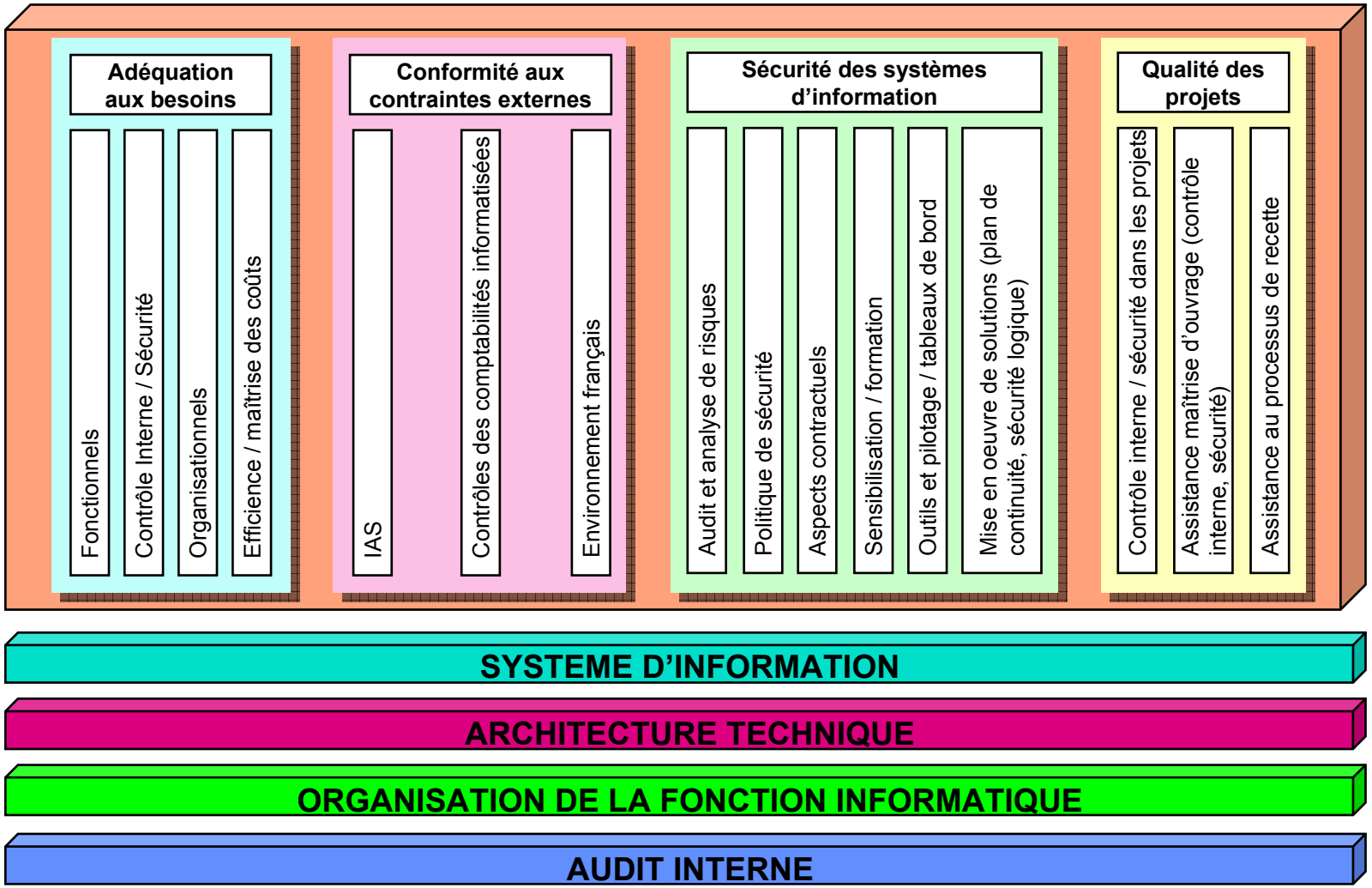
La sécurité		**L'efficience**
Des systèmes :	Des opérations :	Efficacité
Disponibilité Intégrité Confidentialité	Exhaustivité Validité Comptabilisation Séparation des exercices Evaluation Présentation	Evolutivité Maîtrise des coûts

De **l'audit de sécurité / contrôle interne** **à** **l'audit OPERATIONNEL**

Les caractéristiques de la démarche

- Progressive
  - Différents objectifs successifs
- Modulaire
  - Application en tout ou partie
- Universelle
  - Tous les domaines potentiellement concernés par l'audit
- Opérationnelle
  - Orientée vers la proposition de solutions concrètes

En résumé


Adéquation aux besoins
Fonctionnels
Contrôle Interne / Sécurité
Organisationnels
Efficience / maîtrise des coûts
Conformité aux contraintes externes
IAS
Contrôles des comptabilités informatisées
Environnement français
Sécurité des systèmes d'information
Audit et analyse de risques
Politique de sécurité
Aspects contractuels
Sensibilisation / formation
Outils et pilotage / tableaux de bord
Mise en oeuvre de solutions (plan de continuité, sécurité logique)
Qualité des projets
Contrôle interne / sécurité dans les projets
Assistance maîtrise d'ouvrage (contrôle interne, sécurité)
Assistance au processus de recette
SYSTEME D'INFORMATION
ARCHITECTURE TECHNIQUE
ORGANISATION DE LA FONCTION INFORMATIQUE
AUDIT INTERNE

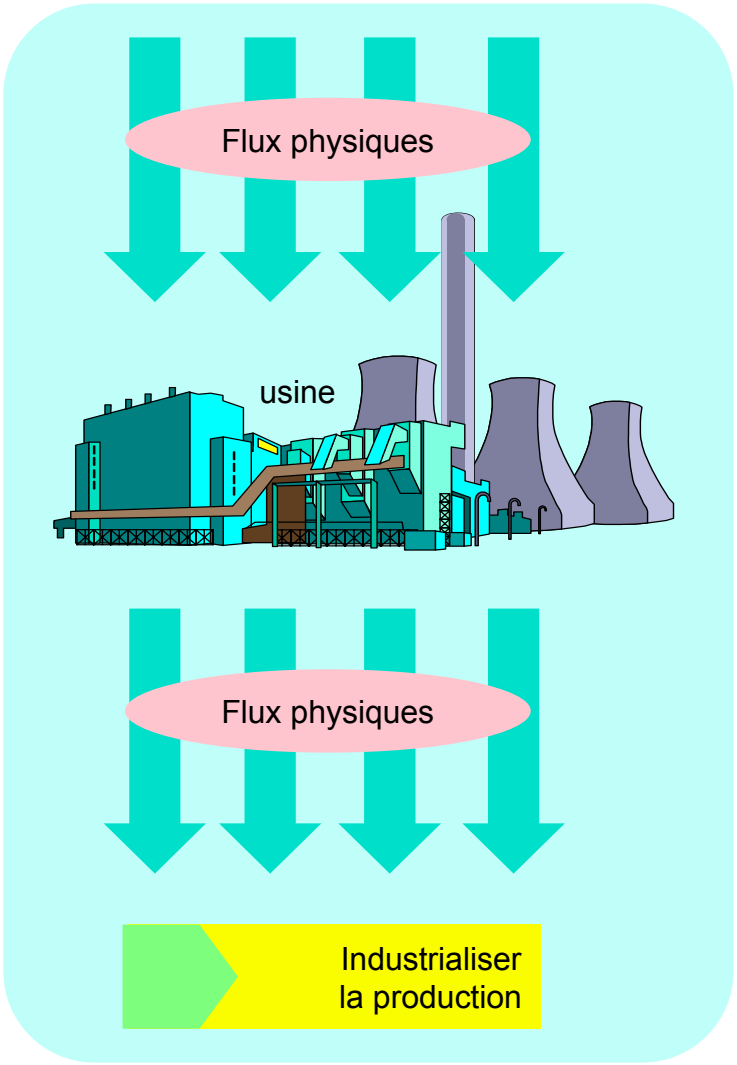
L'audit d'application

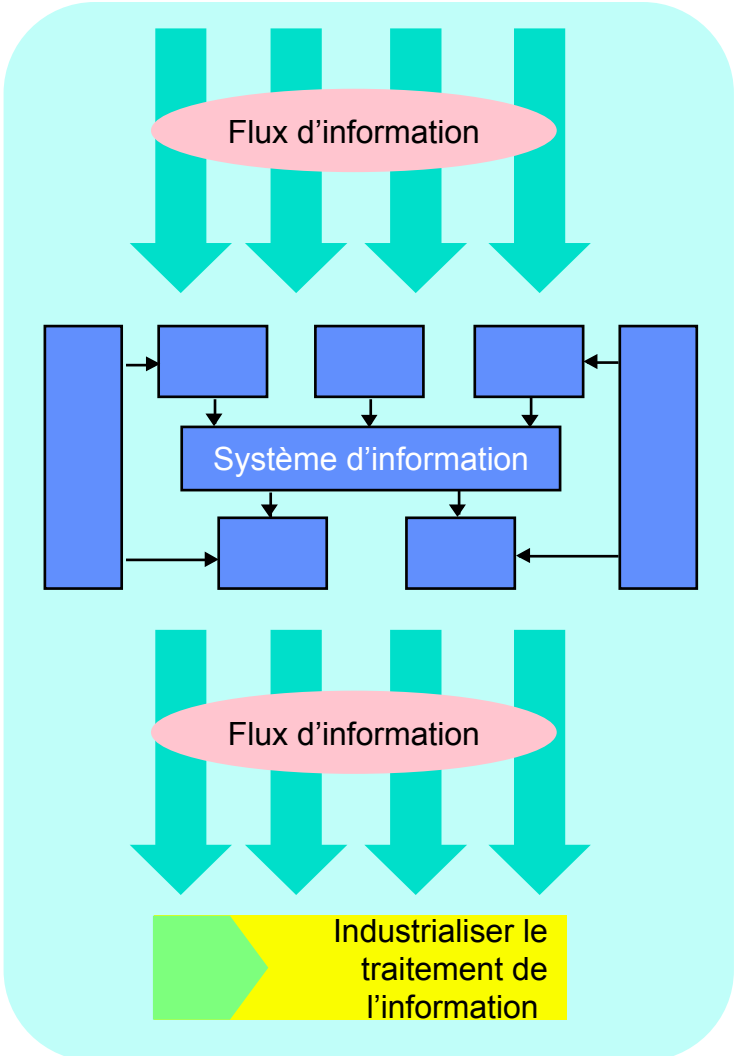
Audit fonctionnel
(ou d'application)

- Les systèmes d'information ➔
- La démarche d'audit d'une application ➔

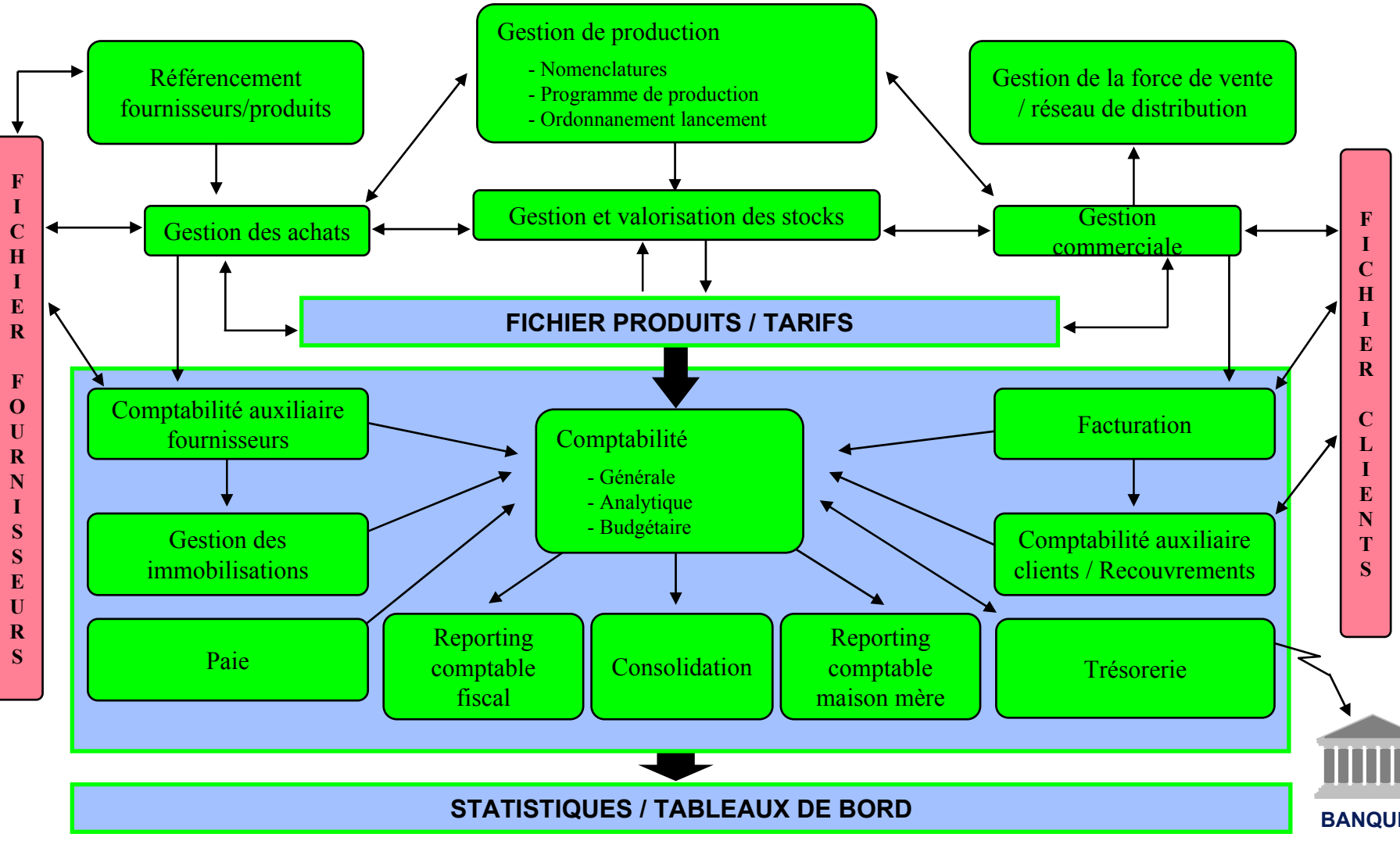
LES SYSTEMES D'INFORMATION

Le système d'information dans l'entreprise





Le système d'information dans l'entreprise



Les enseignements du système d'information (1/4)

- Évaluation de l'architecture du système d'information
  - Degré d'informatisation des processus
  - Degré d'intégration des traitements
  - Structuration des données (ex : unicité de la base clients)
  - Cohérence des informations comptables, réglementaires et de gestion
  - Part des traitements micro-informatiques
  - Part des traitements externes

Les enseignements du système d'information (2/4)

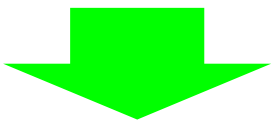
- Évaluation de la cohérence avec les objectifs de l'organisation
  - Politique générale
  - Schéma directeur
  - Directives du Groupe
  - Évolution des activités
  - Évolutions du contexte institutionnel, légal, réglementaire
  - Évolution technologique

Les enseignements du système d'information (3/4)

- La délimitation des domaines applicatifs : champ de l'audit
  - Applications de collecte des opérations (saisie, supports magnétiques, vidéotex...)
  - Applications de traitement des opérations (gestion administrative, comptabilité)
  - Applications de restitution/diffusion des résultats (routage...)
  - Gestion des données permanentes (base clients, produits)
  - Applications "techniques" (interpréteur, interface de transmission de fichiers, gestion de la confidentialité...)

Les enseignements du système d'information (4/4)

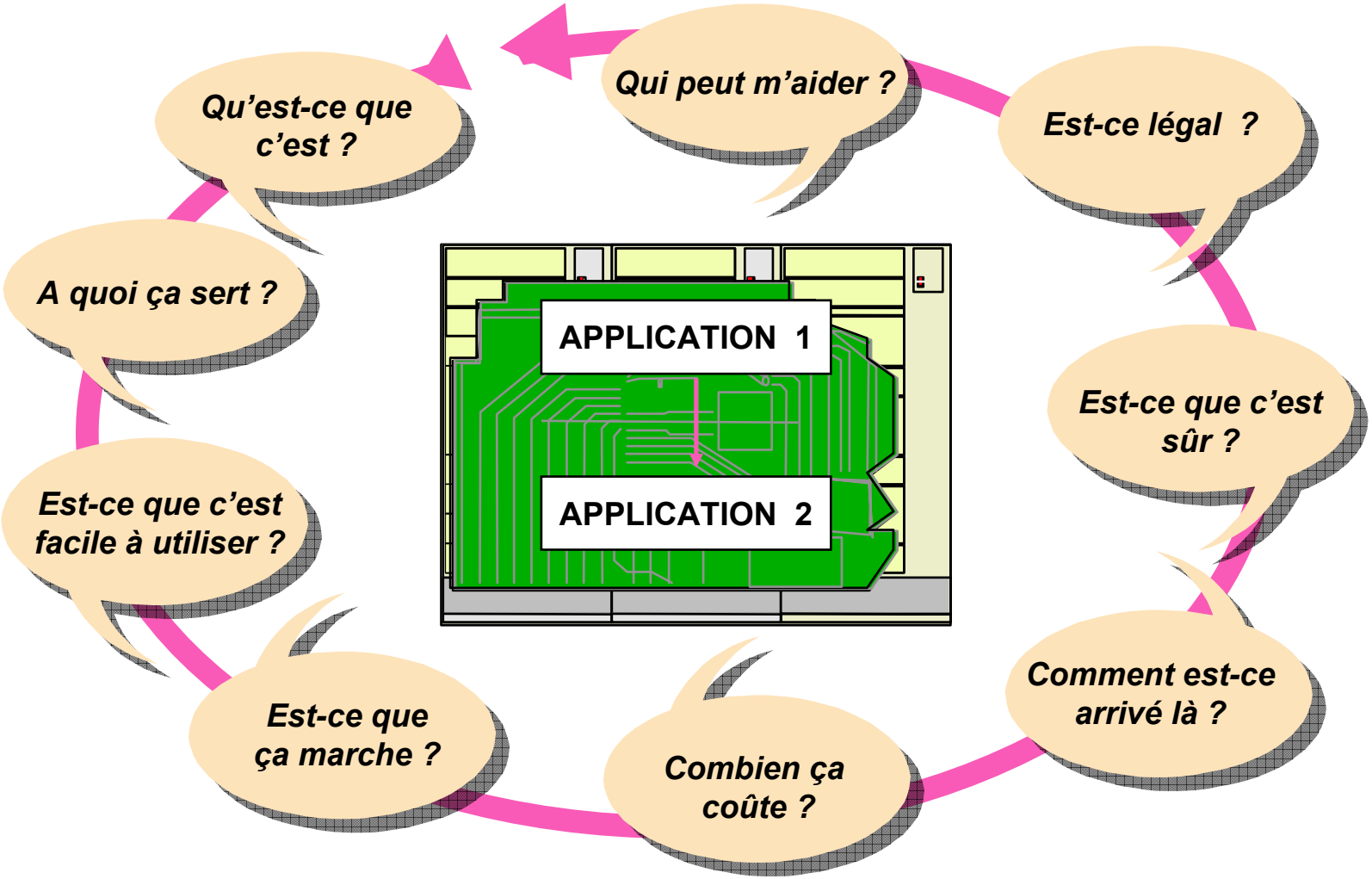
- La délimitation des domaines auditables
  - Par activité ou processus (de l'initiation d'une catégorie d'opérations à la comptabilisation)
  - Par direction / service
  - Par entité géographique
  - Par environnement technique



  - Définition des enjeux et des priorités
  - Organisation des travaux d'audit

LA DEMARCHE D'AUDIT D'UNE APPLICATION

Présentation de la démarche



Présentation de la démarche

- Etapes de la démarche
  - Prise de connaissance
  - Evaluation des enjeux
  - Evaluation fonctionnelle
  - Evaluation technique
  - Evaluation financière
  - Evaluation de la conduite de projet
  - Evaluation de la sécurité et des contrôles internes des traitements
  - Evaluation du support aux utilisateurs

Présentation de la démarche : prise de connaissance

- Interlocuteurs
  - Direction utilisatrice / Responsable service utilisateur
  - Chef de projet études informatiques
- Points clés à examiner
  - Structures (connaissance de l'activité, équipe, historique, plate-forme technologique...)
  - Modes opératoires (procédures manuelles et automatisées, règles de gestion...)
  - Sécurité

Présentation de la démarche : évaluation des enjeux

- Interlocuteurs
  - Direction Générale
  - Direction utilisatrice
  - Direction informatique
- Points clés à examiner
  - Importance du domaine applicatif pour l'organisation
  - Impact potentiel de la concrétisation d'un risque grave

Présentation de la démarche : évaluation fonctionnelle

- Interlocuteurs
  - Direction utilisatrice / Responsable du service utilisateur
  - Autres utilisateurs : tiers (réclamations), direction comptable, contrôle de gestion, audit interne
  - Chef de projet études informatiques
- Points clés à examiner
  - Adéquation fonctionnelle / État de l'art
  - Adéquation fonctionnelle / Besoins utilisateurs
  - Évolutivité fonctionnelle

Présentation de la démarche : évaluation technique

- Interlocuteurs
  - Chef de projet études informatiques
  - Responsable exploitation informatique
  - Direction utilisatrice / Responsable du service utilisateur

- Points clés à examiner
  - Évolutivité technique
  - Qualité des résultats fournis / Normes de service
  - Performance de l'outil
  - Niveaux et taux de service

Présentation de la démarche : évaluation financière

- Interlocuteurs
  - Responsable du suivi des coûts informatiques
  - Responsable du service utilisateur
  - Contrôle de gestion
- Points clés à examiner
  - Rentabilité de l'application
  - Adéquation des modalités de refacturation des coûts aux utilisateurs (le cas échéant)

Présentation de la démarche : évaluation de la conduite de projet

- Interlocuteurs
  - Chef de projet études informatiques
  - Responsable du service utilisateur
  - Direction Générale, utilisatrice et informatique
  - Autres membres de l'équipe de projet
- Points clés à examiner
  - Pertinence des normes, procédures et outils de conduite de projet mis en oeuvre
  - Participation de toutes les personnes clés à la conduite du projet

Présentation de la démarche : évaluation de la sécurité et du contrôle interne des traitements

- Interlocuteurs
  - Chef de projet études informatiques
  - Responsable du service utilisateur
  - Responsable de la sécurité informatique
- Points clés à examiner
  - Correcte mise en oeuvre des contrôles généraux informatiques dans le domaine applicatif concerné
  - Mise en oeuvre de l'approche par les risques sur les principaux processus et traitements

Présentation de la démarche : évaluation du support aux utilisateurs

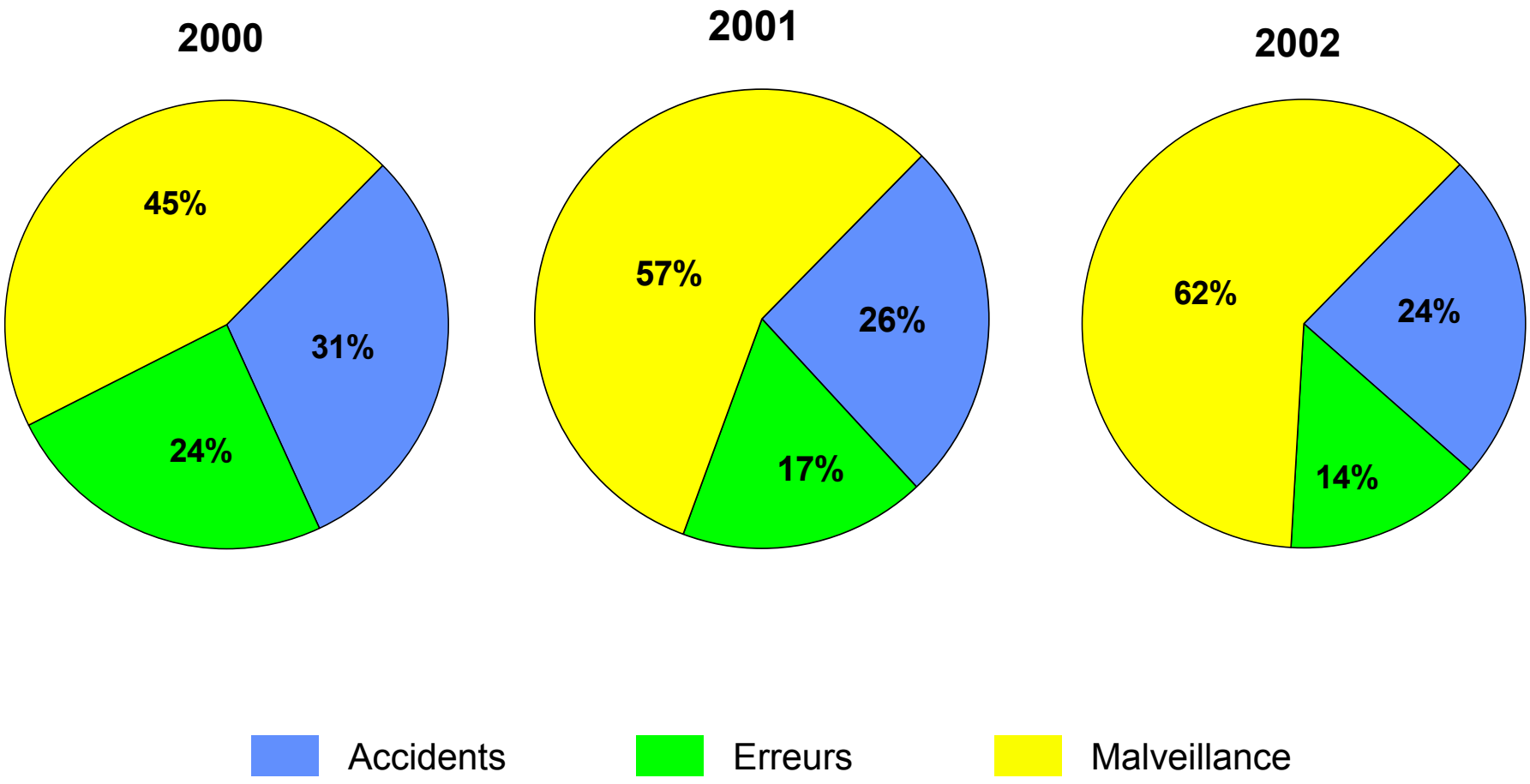
- Interlocuteurs
  - Responsables du support utilisateur au sein de la Direction Informatique
  - Responsable du service utilisateur
- Points clés à examiner
  - Qualité de l'aide documentaire disponible (manuels, en ligne)
  - Support fonctionnel
  - Support technique
  - Qualité de l'assistance fournie en cas d'incidents

Audit des Fonctions Informatiques

- Sécurité des systèmes d'information ➔
- Procédures d'exploitation ➔

SECURITE DES SYSTEMES D'INFORMATION

L’audit de fonctions informatiques



ource : CLUSIF

L'audit de fonctions informatiques

MENACES LOGIQUES

HUMAINES

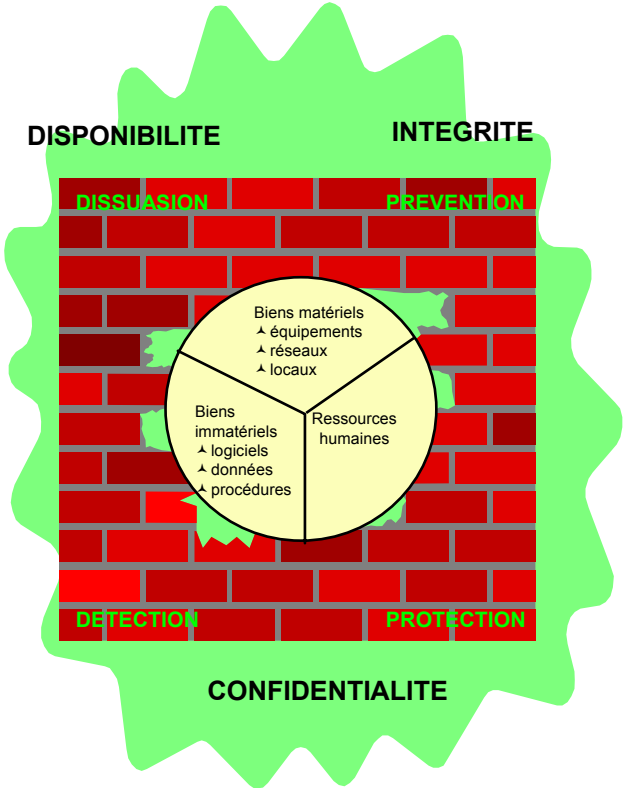
Volontaire :
- malveillance
- vol
- sabotage
- vol d'information
- copie illicite

Involontaire :
- erreur d'exploitation
- erreur d'utilisation

NON HUMAINES

Panne :
- dysfonctionnement logiciel

Accident :
- incendie entraînant l'altération des ressources



ENVIRONNEMENT INTERNE

Volontaire :
- malveillance
- vol
- sabotage
- détournements de ressources

Involontaire :
- destruction du matériel par erreur

Panne :
- dysfonctionnement matériel

ENVIRONNEMENT EXTERNE

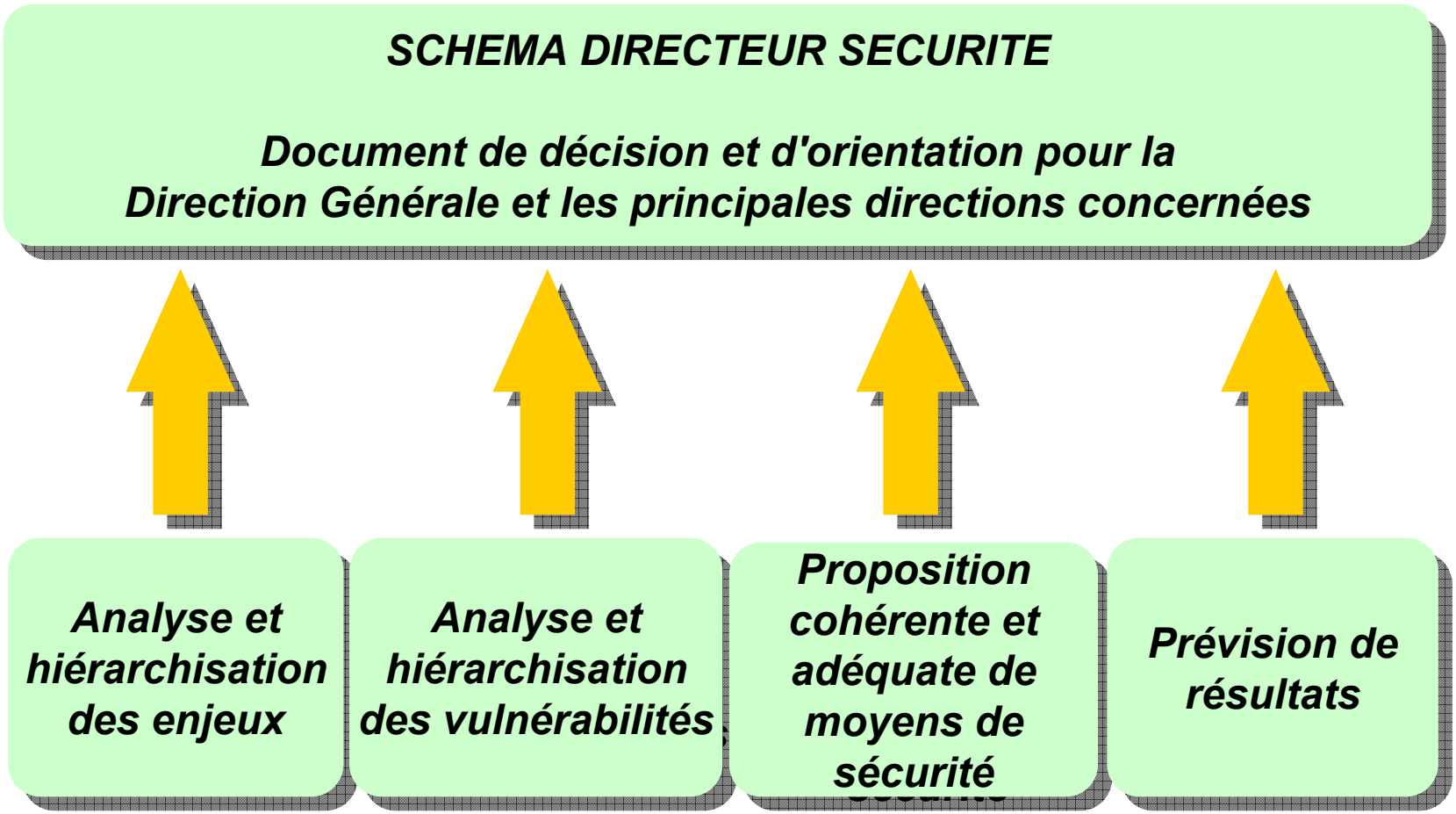
Accidents :
- incendie
- inondation
- orage, foudre
- avalanche
- pollution, vibrations
- perturbations électriques ou électromagnétiques

MENACES PHYSIQUES

Audit de l'organisation de la sécurité

- Objectifs :
  - s'assurer que la sécurité du système d'information est une préoccupation permanente de la direction de l'entreprise et que dans ce cadre, il existe une politique, formellement définie au niveau de l'entreprise, connue de tous les acteurs et appliquée
  - vérifier que l'organisation mise en place permet d'appliquer de façon efficace les orientations fixées par la direction
- Approche d'audit :
  - appréciation de la politique de l'entreprise
  - appréciation de l'organisation générale
  - contrôle de l'organisation opérationnelle
  - contrôle de l'existence des procédures

Schéma directeur sécurité



Exemple de contenu d'un schéma directeur sécurité (1/2)

- Notions générales et domaine d'application
- Contrôle des accès
- Personnel
- Matériel
- Service technique
- Logiciel de base
- Développement du système

Exemple de contenu d'un schéma directeur sécurité (2/2)

- Logiciels d'application
- Sécurité des données
- Traitement automatique des données
- Protection contre les risques naturels
- Stockage externe
- Solution de secours
- Assurances

Contenu-type d'un tableau de bord de sécurité informatique

TABLEAU DE BORD SECURITE

SECURITE GENERALE

- Suivi du schéma directeur sécurité, des actions de sécurité
- Suivi de l'évolution des risques liés à la structure du personnel

SECURITE PHYSIQUE

- Nombre d'accès (création de badges), de vols et fraudes, ...
- Disponibilité des matériels, interruptions, durée de maintien

SECURITE LOGIQUE

- Gestion du logiciel de contrôle (création / suppression des identifiants, ...)

FIABILITE DU S.I.

- Nombre d'anomalies par activité, respect du planning,
- Maintenance (nombre et durée des dépannages, ...)

CONTROLE

- Nombre de réclamations
- Nombre de mots de passe refusés, nombre de déconnexions, ...

Points à examiner (1/2)

- Existence d'une fonction dédiée à l'administration de la sécurité informatique
- Position de la fonction d'administration de la sécurité informatique dans l'organisation (rattachement au responsable de la sécurité générale ?)
- Indépendance de la fonction sécurité par rapport aux opérationnels et par rapport à la DSI (rattachement de la fonction sécurité informatique au responsable de la sécurité générale ?)
- Qualification du responsable de la sécurité informatique

Points à examiner (2/2)

- Existence d'une stratégie claire en matière de sécurité informatique (déclinaison du schéma directeur informatique en schéma directeur sécurité)
- Cohérence de la sécurité informatique par rapport au plan de sécurité générale
- Existence d'outils de mesure du niveau de sécurité (tableaux de bord, audits périodiques)
- Existence d'un reporting sécurité à la Direction Générale, effectivement pris en compte

La sécurité physique

- Analyse critique de la sécurité des sites informatiques
- Analyse critique des procédures de sauvegarde

Analyse critique de la sécurité des sites informatiques

Identification des sites à protéger

- Salle machine
- Locaux techniques
  - climatisation
  - secours électrique
  - autocommutateur
  - têtes de lignes réseau
- Locaux informatiques
  - salle console système
  - bureaux exploitation
  - bureaux d'étude
- Locaux d'archive
  - bandothèque
  - documentation études / exploitation
- Locaux informatiques répartis (informatique de production / départementale)

Identification des menaces

- Liées à l'environnement général (proximité de sites potentiellement dangereux)
- Liées à l'agencement des locaux (canalisations souterraines, passages de lignes électriques)
- Liées au facteur humain (grève, émeute, sabotage)
- Accidentelles (incendie, dégâts des eaux)
- Catastrophes naturelles

Recensements des mesures de protection

- Sécurité des accès physiques
- Incendie
- Dégâts des eaux
- Alimentation électrique
- Environnement adéquat

Evaluation forces / faiblesses

- Adéquation mesures de protection / menaces
- Fréquence et qualité des tests et mesures de protection
- Nature et ampleur des menaces non couvertes

Analyse critique de la sécurité des sites informatiques (1/3)

- Accès physiques
  - Pour les locaux informatiques
    - emplacement du site et des locaux
    - protection physique des accès (blindage, etc...)
    - contrôle des accès du personnel (badge, code d'accès, ...)
    - système de surveillance
  - Pour les accès physiques aux terminaux répartis
    - installations de systèmes de clés physiques, de fixation, ...

Analyse critique de la gestion de la sécurité logique (2/3)

- Stratégie de sécurité logique :
  - l'identification des ressources et des données à protéger
  - la classification de celles-ci
  - l'appréhension des risques
  - l'identification et le suivi des utilisateurs
  - la mise en place du système de protection des accès
  - le suivi de l'utilisation des outils

Analyse critique de la sécurité des sites informatiques (3/3)

- Régulation de l'alimentation électrique
  - onduleur
  - groupe électrogène
- Maintien d'un environnement adéquat
  - température
  - hygrométrie
  - filtrage de l'air
  - climatisation de secours

Analyse critique des procédures de sauvegarde

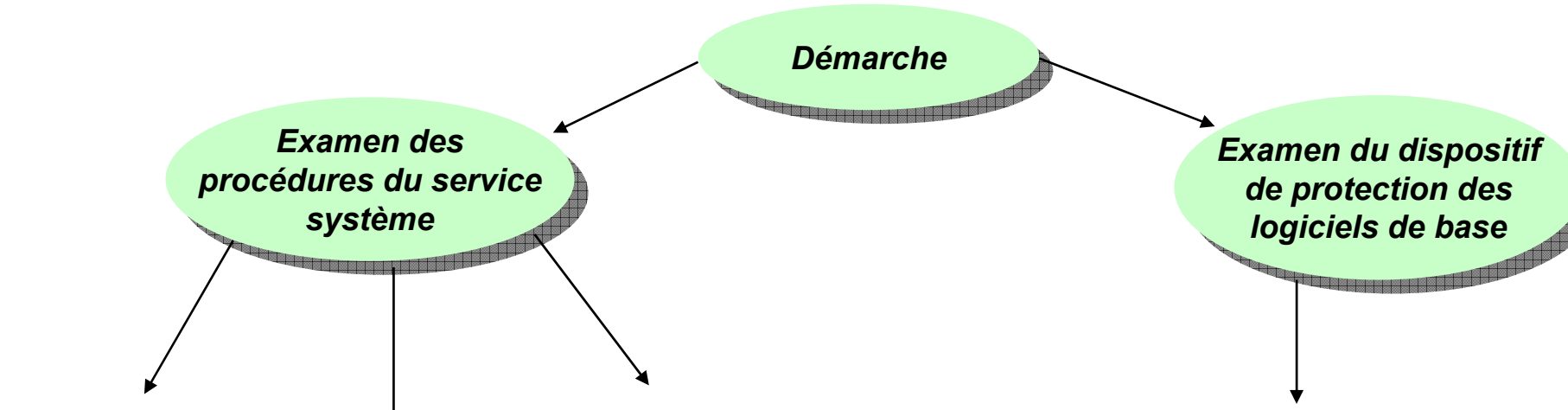
- Points clés à examiner
  - Ressources sauvegardées incomplètes
  - Périodicité des sauvegardes trop espacées
  - Lieu de stockage non protégé
  - Procédures de sauvegardes / restauration non formalisées et non testées
  - Sauvegardes non fiables

PROCEDURES D'EXPLOITATION

Attribution des responsabilités (3/3)

- Le propriétaire de l'application doit :
  - s'assurer que l'ensemble des éléments nécessaires au transfert est effectivement rempli
  - s'assurer que les différentes revues relatives à la sécurité, à la protection des données ont été réalisées, que leurs résultats ont été formalisés et qu'elles ont été transmises au responsable du projet
  - valider et établir le contrat de service final entre les utilisateurs, les études et la production

Domaine système : enjeux



- Procédures formalisées
- Séparation des fonctions
- Documentation
- Supervision des travaux

- Gestion des logiciels de base (système et réseau)
- Gestion des incidents
- Réalisation de développements spécifiques

- Protection des données
- Protection des programmes
- Journalisation

- Maintenance des systèmes :
  - changement de système
  - nouvelles versions
  - changement de matériels
- Initialisation du système :
  - arrêt machine
  - maintenance matériel
  - maintenance logiciels de base
- Maintenance des logiciels de base :
  - ajout de nouvelles fonctions
  - modification de paramètres
  - correction d'anomalies spécifiques