ubizen

we secure e-business

Normes ISO
Gestion des risques: Guide 73
Sécurité des S.I.: 13335

Club EBIOS

16 Mars 2004

Ing. JL Allard, CISM, CISA

ISO Guide 73

we secure e-business

Couverture

Concepts

Définitions

1. Couverture

ubizen
we secure e-business

Tous domaines où le Risque est concerné

- Feu
- Blessures
- Projets
- TIC
- Etc.

Donne une approche générique et cohérente, pas une conduite précise pour tous usages

- Il faut “ajouter” des éléments
- Il fut “affiner” les concepts et définitions

1. Couverture 2

we secure e-business

Structure

- Termes de base
- Termes relatifs aux pesonnes et organisations
- Termes relatifs à l'Evaluation des risques
- Termes relatifs au Traitement et au contrôle du risque

Définitions

8 + 4 + 6 + 11 = 29

2. Concepts

ubizen
we secure e-business

Les risques doivent être

- Identifiés
- Estimés
- Comparés à des “Critères de Risque”

Les risques Evalués doivent être

- Acceptés ou Traités
- Communiqués
- Revus

3. Définitions 1

we secure e-business

Evaluation des Risques =

- Analyse des Risques
  - Identification des Sources
  - Estimation des risques
- Evaluation des Risques

Traitement des Risques =

- Evitement des risques
- Optimisation des risques (Réduction [mitigation])
- Transfert du risque
- Conservation du risque (acceptation)

ubizen
we secure e-business

Le risque est

... La Probabilité qu'

... Un Evènement ait

... Des Conséquences négatives.

4. Limitations

ubizen
we secure e-business

“Lors de la préparation d’une norme qui inclut des aspect de gestion des risques, il faut d’abord faire attention aux définitions de ce guide... Pour développer une compéhension commune parmi les oranisations... Cependant, il peuit s’avérer n”cessaire de dévier des mots exactspour rencontrer les besoins d’un domaine spécifique...”

5. Spécificités des TIC

we secure e-business

Nouveaux concepts:

- *Les évènements se produisent sous formes de scénarios potentiels*
  - ***De la source vers les 'frontières' du système***
  - ***Depuis le 'point d'entrée' vers la 'cible'***
- Les conséquences sont aussi indirectes et intangibles

Nouveaux élément:

- Vulnérabilité
  - **Suite au manque / à la faiblesse des protections.**

“Le” 13335

we secure e-business

GMITS (ISO/IEC TR 13335)

MICTS (ISO/IEC IS 13335)

Gestion des risques

GMITS - MICTS
Introduction

we secure e-business

International Standard Organisation (ISO)

en cooperation avec l'International Electronic Committee (IEC)

Crée une série de normes relatives à la sécurité des technologies de l'information:

- SG1: Management
- SG2: Techniques
- SG3: Evaluation and Certification criteria

GMITS
Qu'est-ce?

ubizen
we secure e-business

Titre: Information Technology - Guidelines for the management of IT Security (GMITS)

en CINQ parties

Pas une norme technique à laquelle se conformer...
... Simplement un Technical Report *(directive)*

Pour donner des recommandations dans le développement et la gestion des politiques de sécurité IT.

GMITS
Contenu

ubizen
we secure e-business

‘***Deux guides sur la Sécurité IT ... pour le Management***’

Part 1: Concepts and models for IT Security (1996)

Part 2: Managing and planning IT Security (1997)

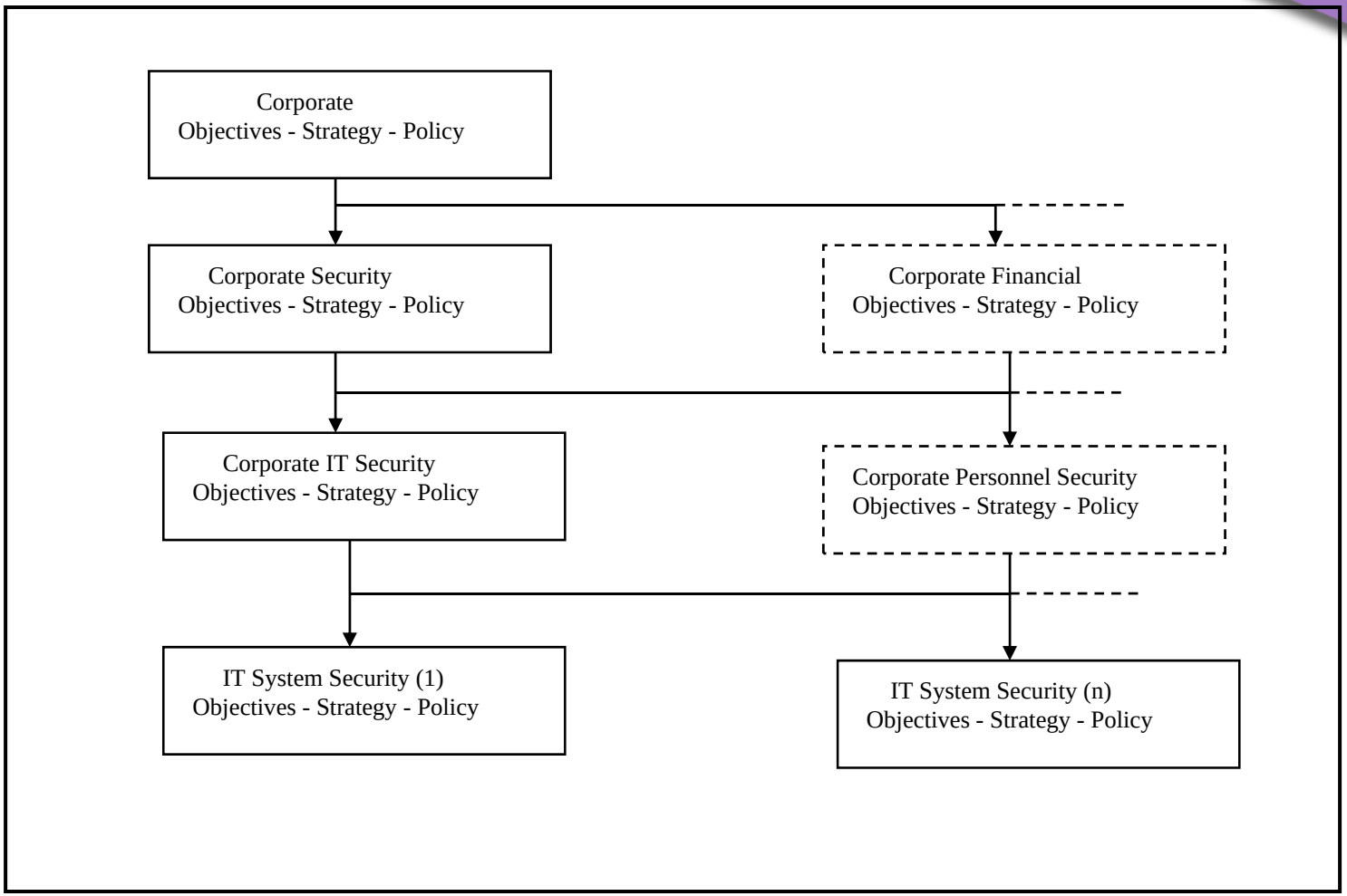
‘***Trois guides pour les IT managers et Security Officers***’

Part 3: Techniques for the management of IT Security (1998)

Part 4: Selection of safeguards (1999)

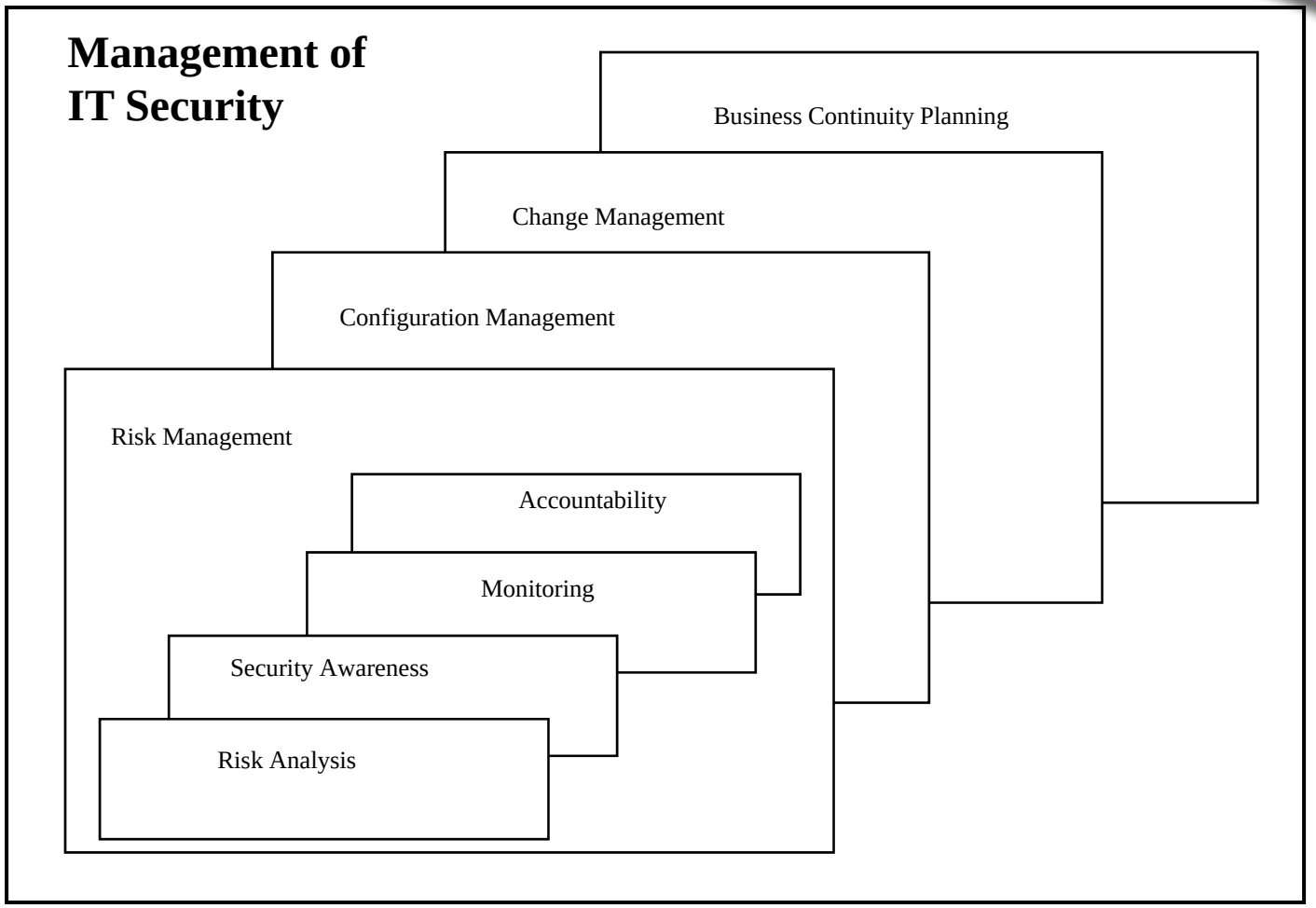
Part 5: Management guidance on network security (fin 2000)

GMITS
Principles (1)

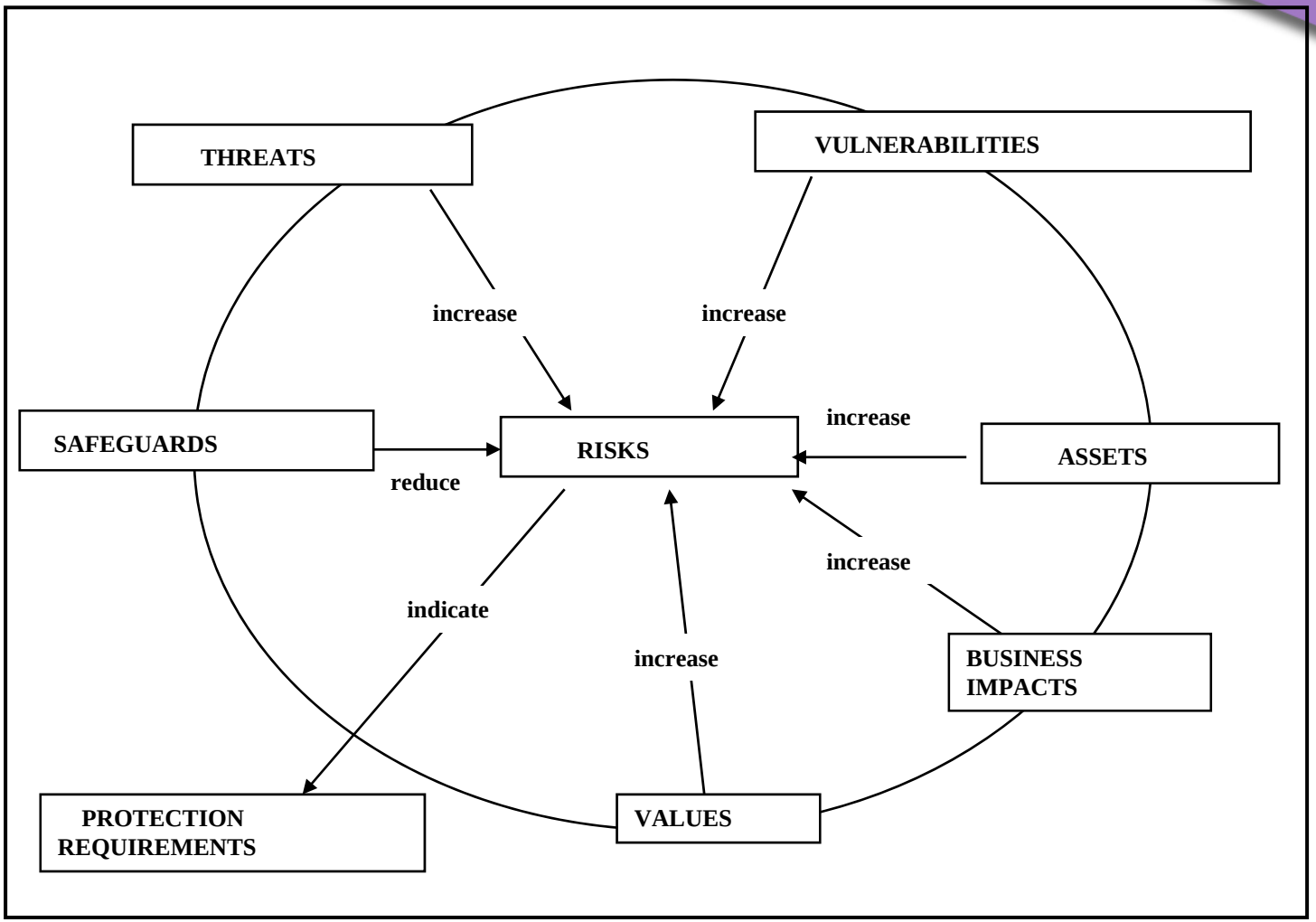


GMITS Principles (2)

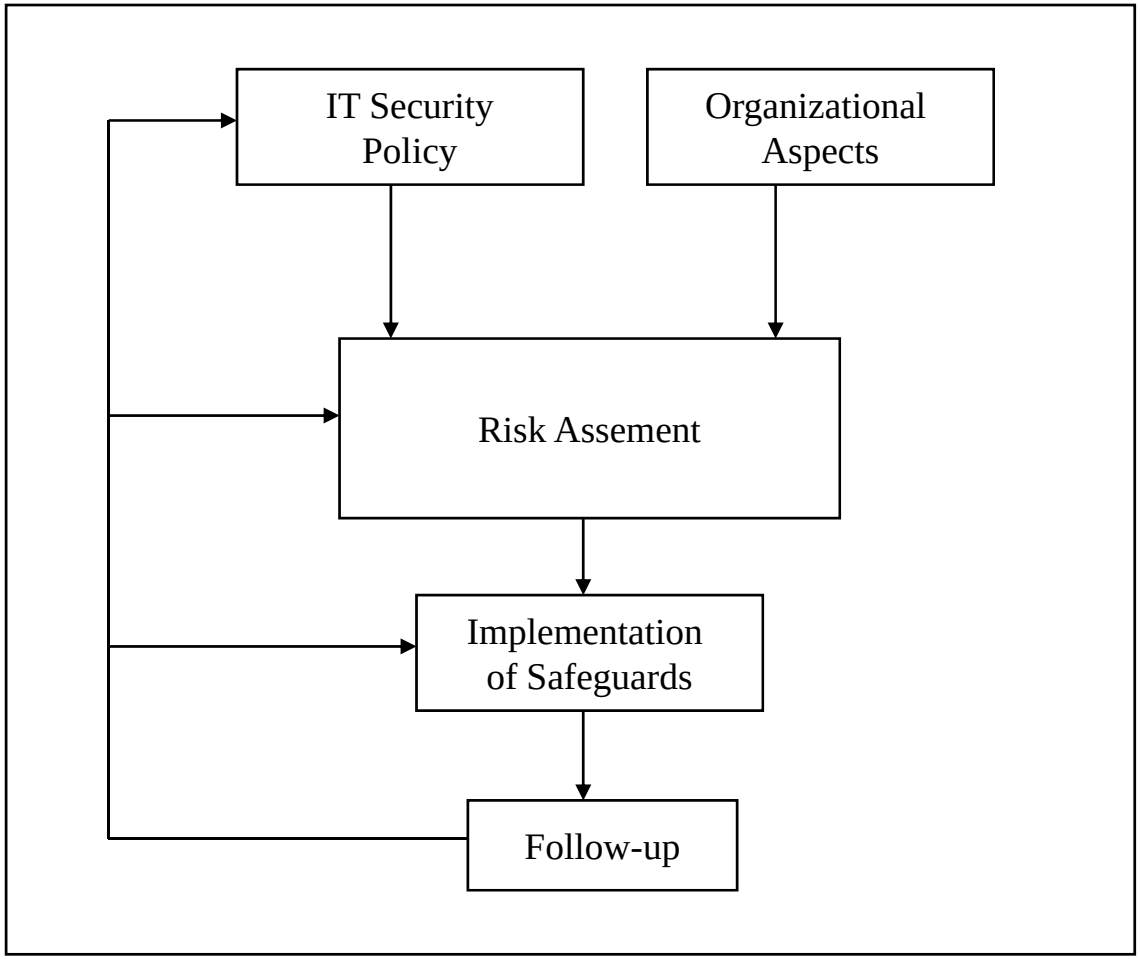
ubizen
we secure e-business



GMITS
Principles (3)



GMITS Principles (4)



MICTS
Qu'est-ce?

we secure e-business

Titre: Information Technology - Management of Information and Communication Technology Security (MICTS)

Une recommandation sous forme d'International Standard' (en parallèle au 17799)

Résultat de la 1ère révision quinquénale du GMITS.

Tient compte de l'évolution du concept de la sécurité des TIC.

Se conforme à l'ISO Guide 73.

MICTS
Contenu

Partie 1:

Remplace les GMITS-1 et -2

Devrait être publié avant la fin de l'année.

Partie 2:

Remplace les GMITS -2, -3 et -4

Demande encore du travail.

Le GMITS-5 sera déplacé vers le 18028 (Network Security) lors de sa révision l'an prochain.

MICTS
Contexte

we secure e-business

Préparer les Politiques de Sécurité des TIC

- entreprise => systèmes

Aider à 'manager' la sécurité des TIC

- définir, planifier, organiser, gérer, maintenir...

Identifier les besoins en sécurité des nouveaux systèmes TIC

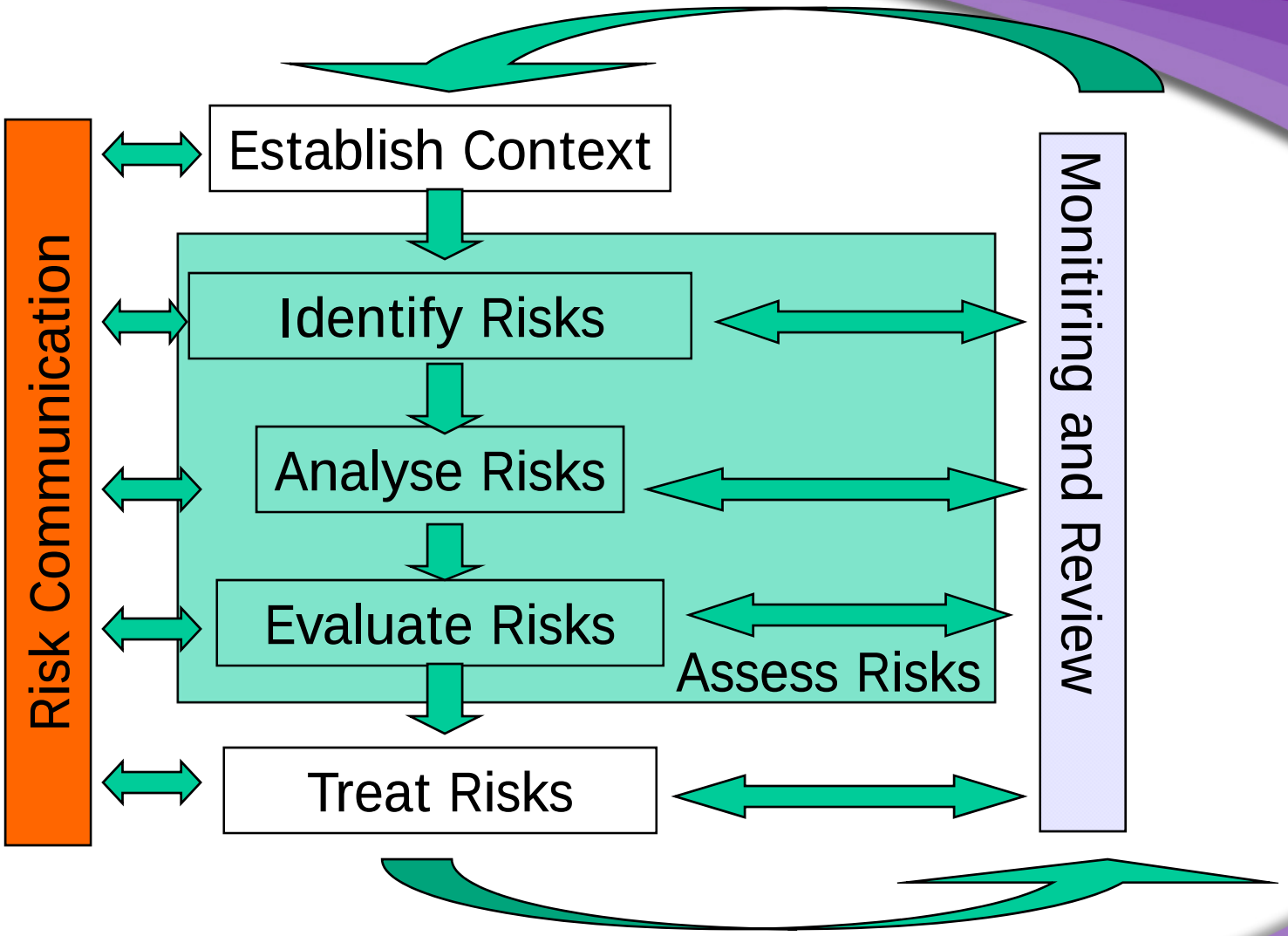
Vérifier que les S.I. actuels sont correctemernt protégés.

MICTS-1
Table des matières

MICTS-2
Table des matières (*draft*)

ubizen
we secure e-business

MICTS-2
Gestion des risques - articulation



MICTS-2
Gestion des risques - Approches

we secure e-business

Baseline

- Bonnes pratiques en cas d'utilisation des TIC dans un contexte défini...
- **Traitement du risque** seulement

High-level risk assessment

- Simplifié & Raccourci
- Focalisé et Rapide
- Diagnostic préliminaire

Detailed risk assessment

- Complète (long et chère)

Combined approach for risk assessment

- Mélange High-level et Detailed

Traitement du risque

- Détaillé (au départ du GMITS-4)

4. ISO/IEC
Travaux WG1 et WG3

ubizen
we secure e-business

WG1

- 15947 - IT intrusion detection
- 17799 - Code of pracxtice for ISMS
- 18028 : IT Network security (same level as BS 7799) [5 parts]
- 18043 - Guidelines for the implementation, operations and management of IT IDS
- 18044 - Information security incident management
- 21827 - System Security Egineering - Capability Maturity Model (SSE-CMM)

WG3:

- 15408 - valuation criteria for IT security [Common Criteria]
- 15443 - A framework for IT security assurance
- 15446 - Guide for the production of protection profiles and security targets
- 18045 - Methodology fot IT security evaluation
- 19791 - Security assessment of Operational Systems