INTERNET SECURITY DAYS
26/03/2007

Connaissez-vous les **risques** de vos **informations**?

Carlo Harpes
itrust consulting s.à r.l.

Objectif

1. Vos informations ont de la valeur !
2. Apprendre les termes clés de l'analyse de risques
3. Pourquoi faire une analyse de risque?
4. Connaître quelques méthodes
5. Pouvoir choisir une approche qui vous convient

Motiver à démarrer ou améliorer
vos analyses de risques

Agenda

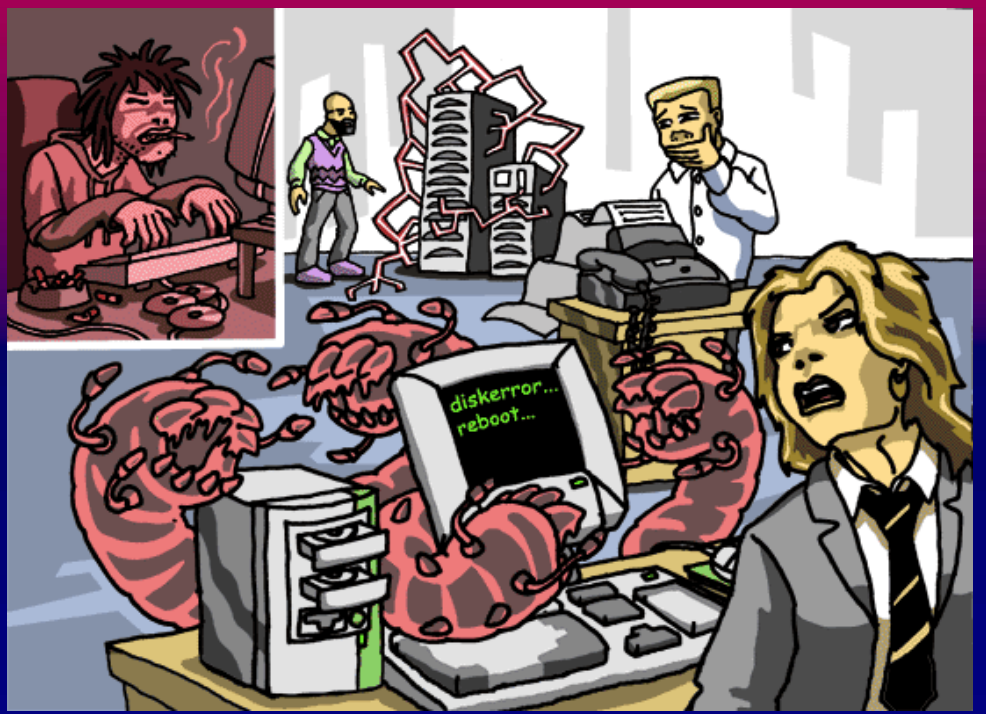
1. Introduction
2. Exercice
3. Terminologie
4. Approche d'analyse de risque
   - ENISA pour PME
   - BSI Grundschutz
   - ISO 27001
5. Conclusion

Risques réels !

itrust consulting s.à r.l.

- 1.200.000 jours: PC hors service après attaque
- 42 % des attaques causées par des Virus
- 10 % des entreprises: soucis avec SPAM ou accès externes

Statistique du BSI à Bonn de 2002



Carthographie

itrust consulting s.à r.l.

Risques légaux

- Protection des données
- Secret bancaire
- Criminalité informatique
- Obligation d'archivage

Risques financiers

- Solvabilité, liquidité
- Risque taux de change
- Mauvaises factures
  ex. EuroCACS: après migration vers SAP, des factures inexistantes ont été payées.

Risques opérationnels

- Mauvaise qualité de service
- Pénalité aux clients
- Dommages

Risques de réputation

- Confiance des clients
- Le plus important – le plus difficile à mesurer

Autres …

Le péché mortel des PME:

itrust consulting s.à r.l.

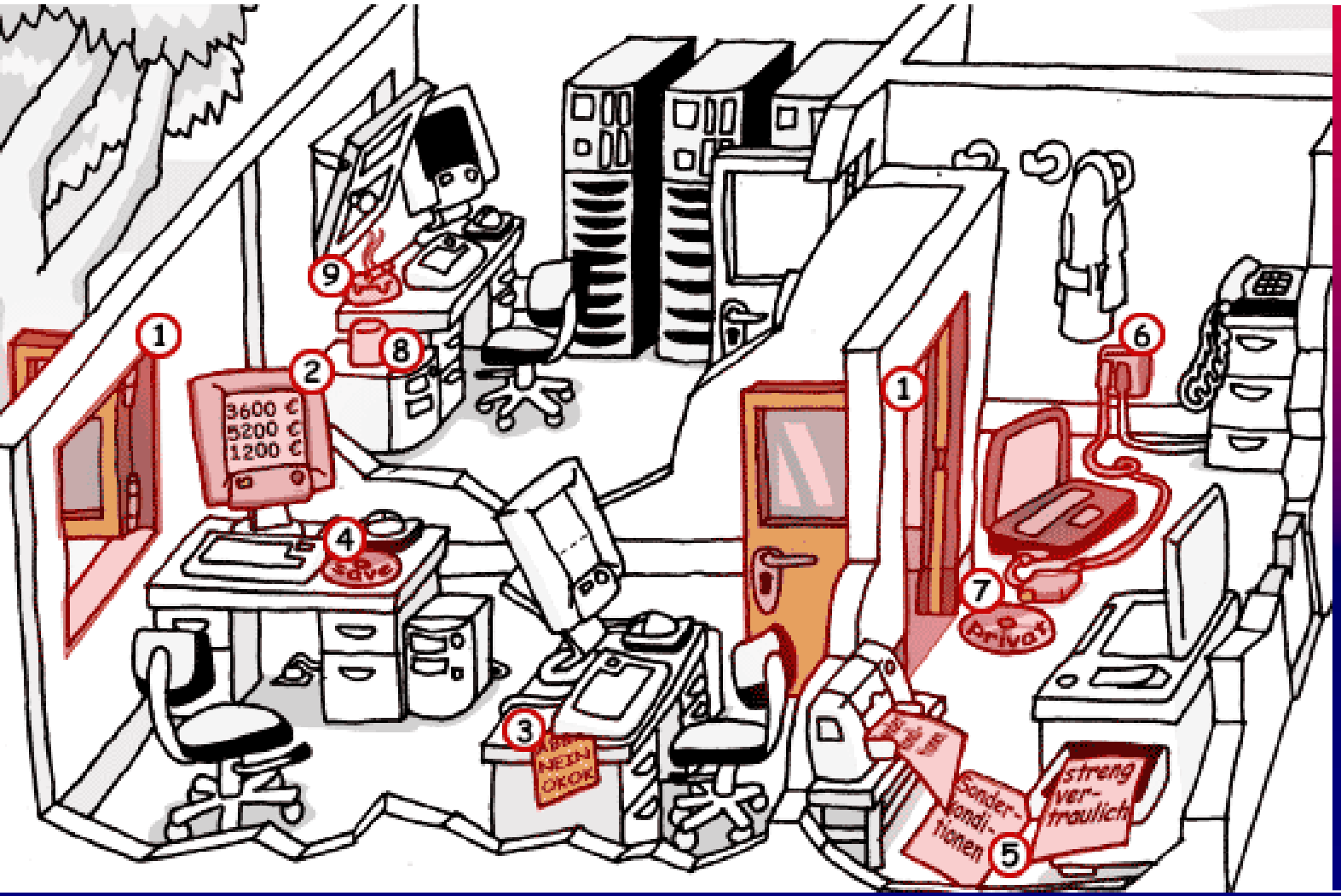
Ceci ne concerne que les grands!

56% des PME ont eu plus d'un incident en 2006

souce ENISA


3600 €
5200 €
1200 €
save
ABR.
NEIN
OKOK
Sonder-
kondi-
tionen
streng
ver-
traulich
privat

Risques réels



1. Fenêtre ouverte
2. Screensaver
3. PWD
4. Backup accessible
5. Doc confidentiel
6. Internet sans FW
7. CD privé
8. Café pour renverser
9. Cigarette

Source BSI

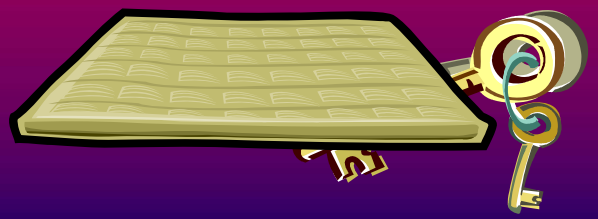
Pourquoi dangereux ?

Avez-vous vraiment le temps de gérer toutes les installations et configurations de sécurité?

Sinon, quels sont les points les plus importants à soigner?

Terminologie

Menace



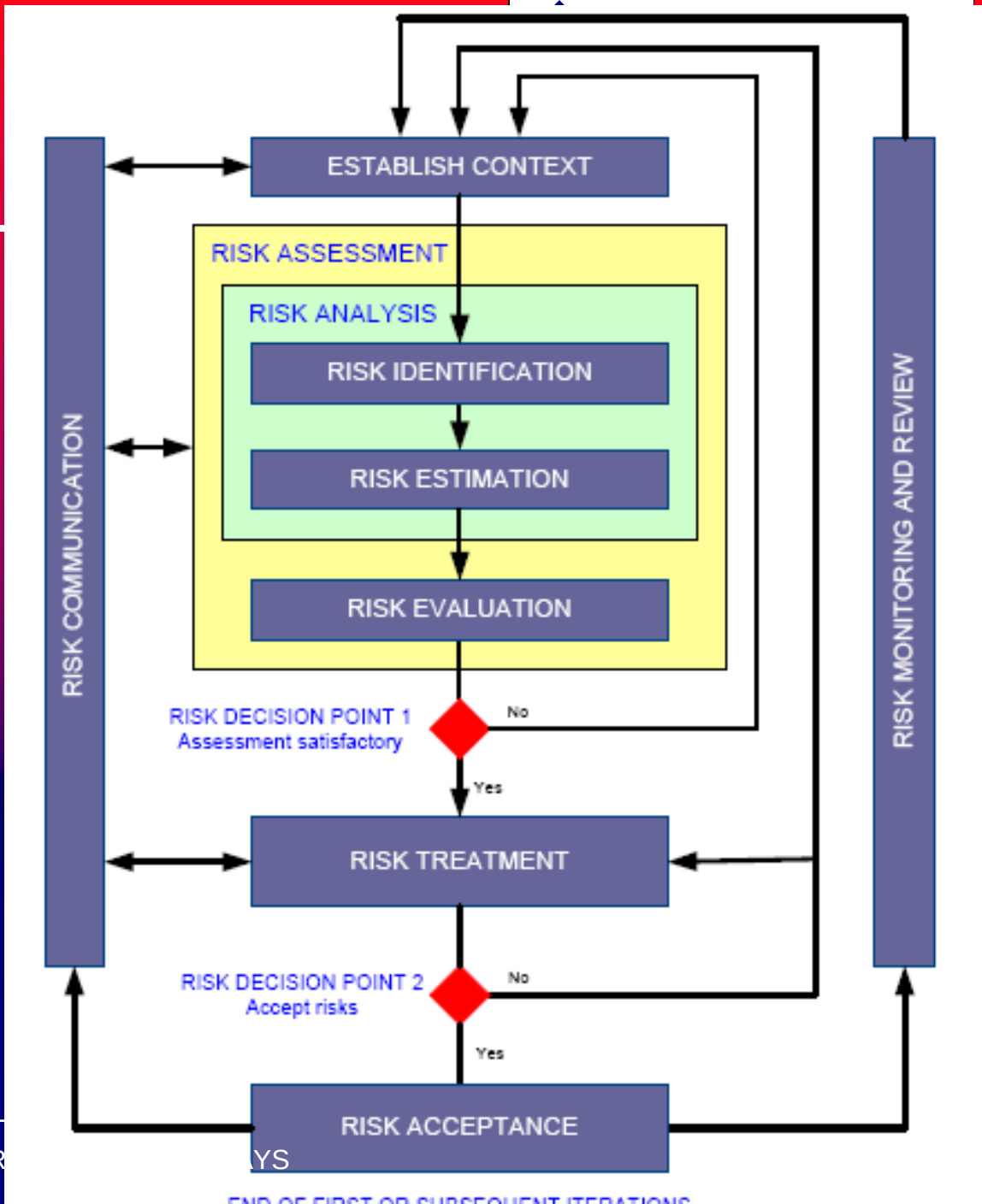
Vulnérabilité

Impact

Risque = Menace • Vulnérabilité • Impact

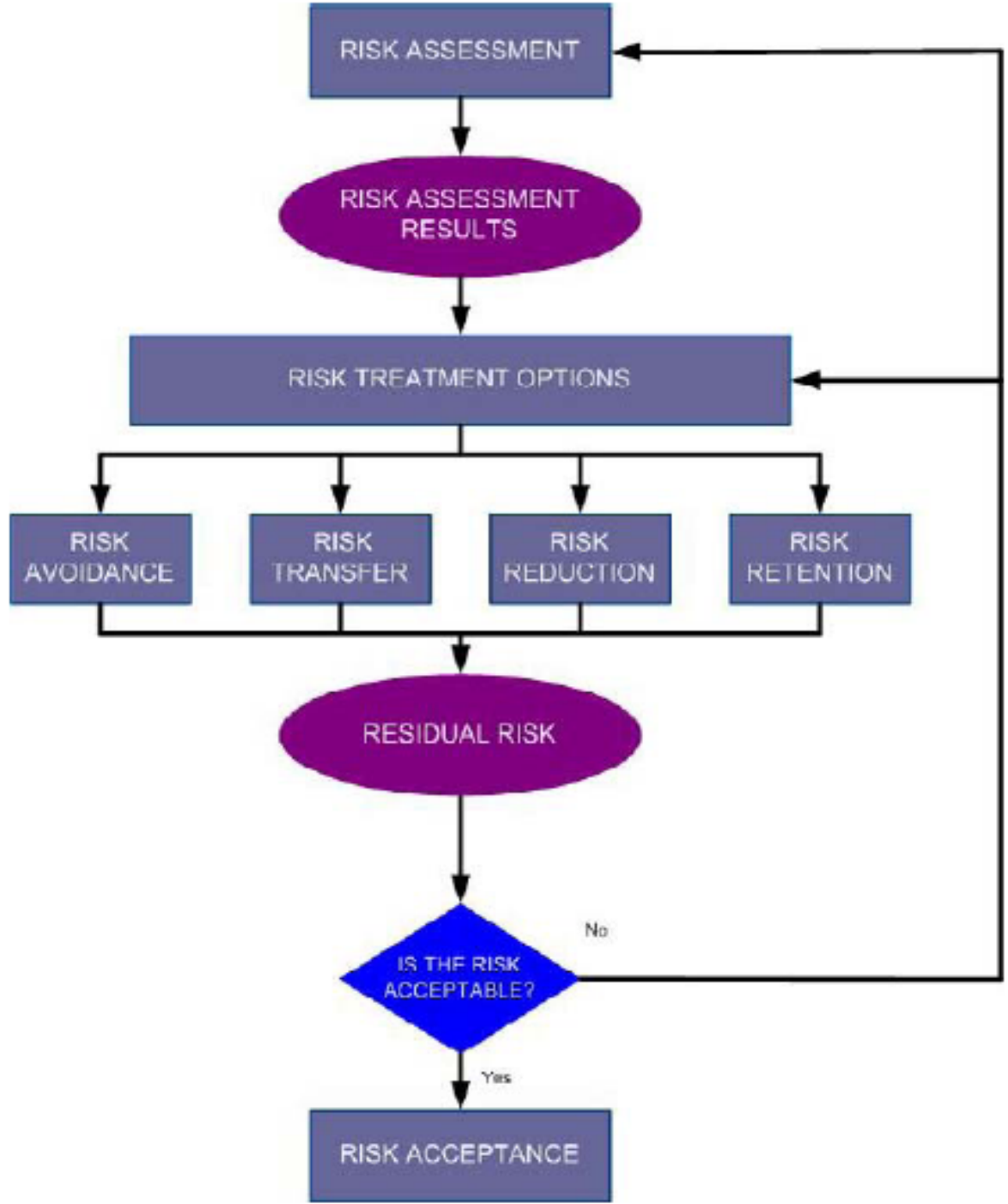
Terminologie:
selon ISO

Le processus d'analyse de risques
selon ISO FCD 27005
(anc. 13335)



Terminologie:
selon ISO

Le traitement des risques selon ISO FCD 27005 (anc. 13335)



Terminologie:
Types de méthodes

itrust consulting s.à r.l.

Méthode qualitative:

> 10 Mio €	2	2	1	1	1
> 1 Mio €	3	2	2	1	1
> 100.000 €	3	3	2	2	1
> 10.000 €	3	3	3	2	1
Insignifiant	3	3	3	3	2
Impact et Fréquence	0.01	0.1	1	10	100

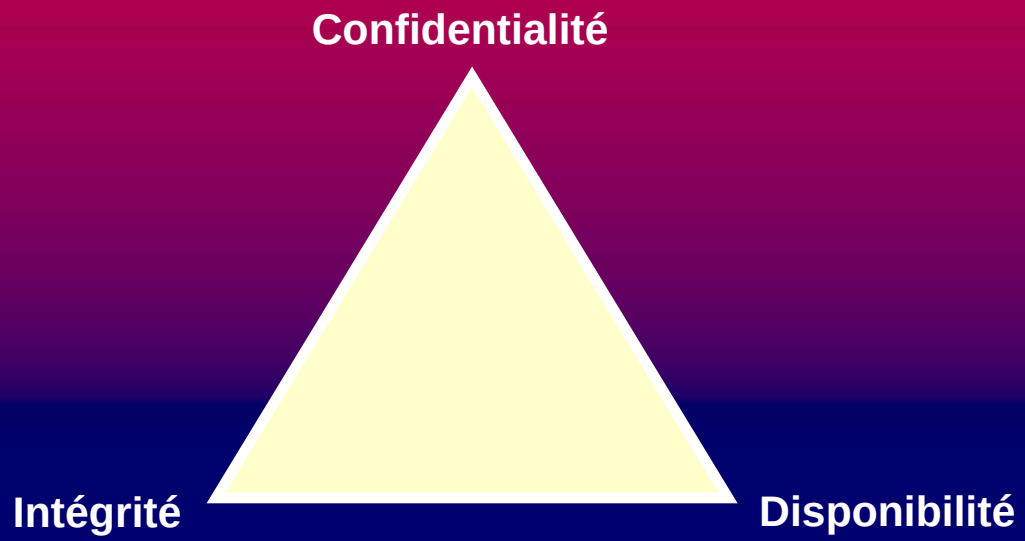
Méthode quantitative:

$$\text{Risque} = \sum \text{Impact / Fréquence}$$

Terminologie:
Valeurs de l'information

itrust consulting s.à r.l.

Critères de sécurité:



Pourquoi analyser les risques ?

itrust consulting s.à r.l.

1. Revoir l'organisation et les technologies
2. Choisir la sécurité en fonction des impacts possibles
3. Focaliser sur l'essentiel
4. Accepter aussi des risques !
5. Assurer l'efficacité de la sécurité en mettant les coûts en relation avec la réduction du risque obtenu

Inhouse ou Outsourcing ?

itrust consulting s.à r.l.

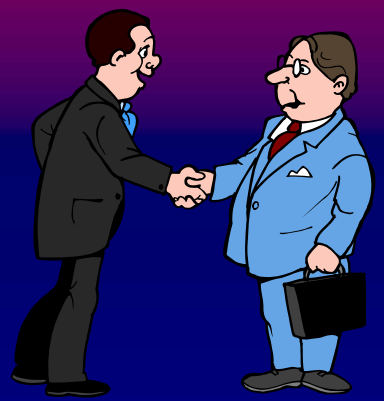
En interne si …

- Petite PME, hiérarchie plate
- Connaissance interne des TIC
- Ressources qualifiées et disponibles
- Peu de dépendances des SI
- Une équipe de 3 personnes avec compétences analytiques, esprit d'équipe, leadership, compréhension business, disponibles plusieurs jours
- Informatique simple, comprise par une personne

En externe si …

- Volonté d'avoir un focus prononcé sur business
- Pas de disponibilité d'une équipe
- Gestion de flux financiers
- Cadre très règlementé

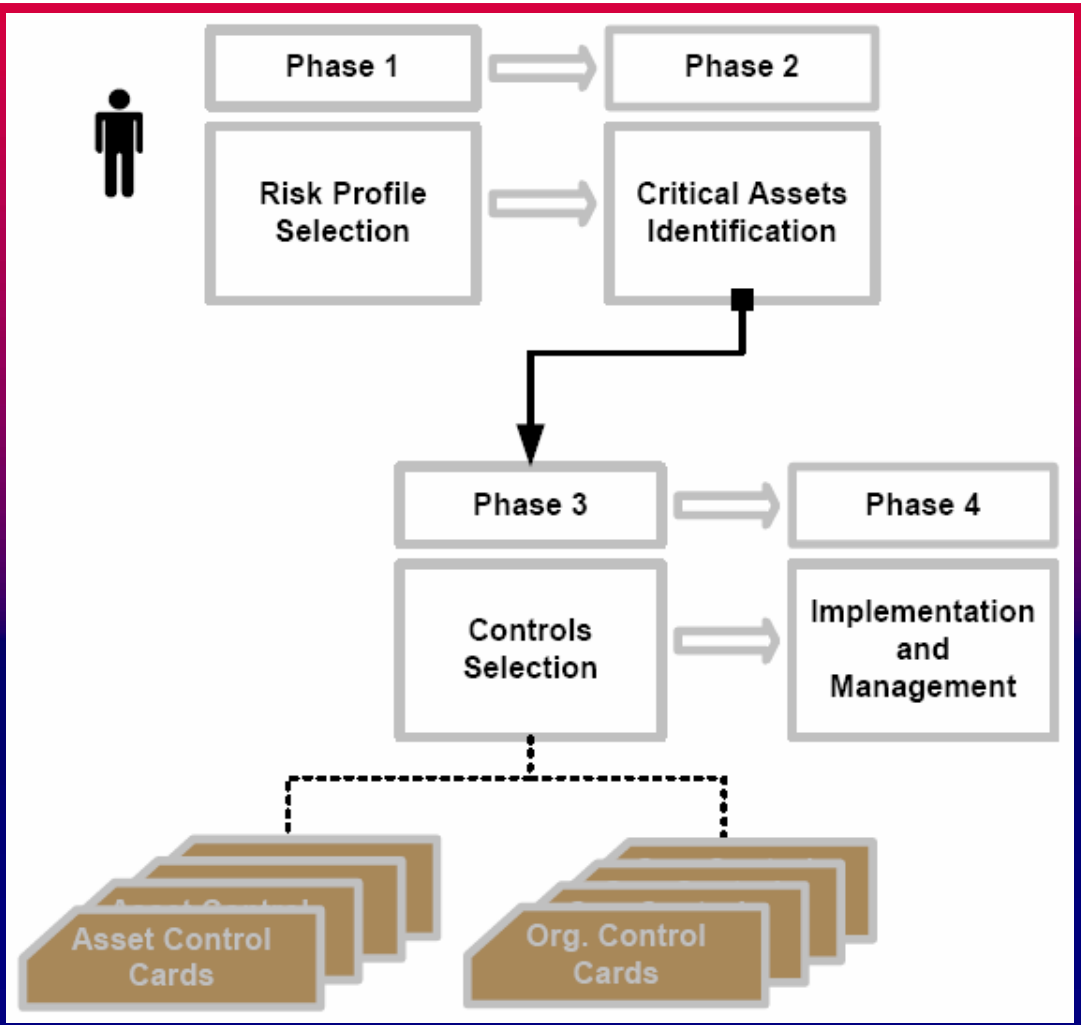
Sinon:



ensemble en partenariat

Source: ENISA

Démarche PME d'ENISA



Démarche PME d'ENISA

itrust consulting s.à r.l.

Phase 1: Sélection de votre profil de risque

- Choisir le niveau High-Medium-Low pour les catégories
  - Cadre légal
  - Productivité
  - Stabilité financière
  - Réputation et confiance clients

Risk Areas	High	Medium
Legal and Regulatory	The organization handles customer information of a sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law.	The organization handles customer information of a personal but not sensitive nature as defined by the EU Data Protection Law.

Démarche PME d'ENISA

Phase 2: Identification et classification des biens et informations critiques

- Identification par catégories
  - Systèmes
  - Réseau
  - Personnel
  - Application
- Classification
  - Confidentialité
  - Intégrité
  - Disponibilité
- Pour les « valeurs » critiques formuler les exigences de sécurité (1-2 phrases)

Démarche PME d'ENISA

itrust consulting s.à r.l.

Phase 3: Sélection du profil de sécurité (Control card selection)

- Mesures organisationnelles
- Mesures pour « asset »

Risk Areas	High	Medium	Low
Legal and Regulatory	(SP1) (SP4)	(SP1) (SP4)	SP1.1

Asset Control Cards			
Asset	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

Démarche PME d'ENISA

itrust consulting s.à r.l.

Asset Based Control Card ID										CC-1A
Risk Profile	High									
Asset Category	Application									
Security Requirements	Physical Security	System and Network Management	System Administration Tools	Monitoring and Auditing IT Security	Authentication and Authorization	Vulnerability Management	Encryption	Security Architecture and Design	Incident Management	General Staff Practices
Confidentiality		2.1.3			2.4.2	2.5.1	2.6.1			
Integrity		2.1.4			2.4.2	2.5.1	2.6.1			
Availability		2.1.6								

Démarche PME d'ENISA

Phase 4: Implémentation et Gestion

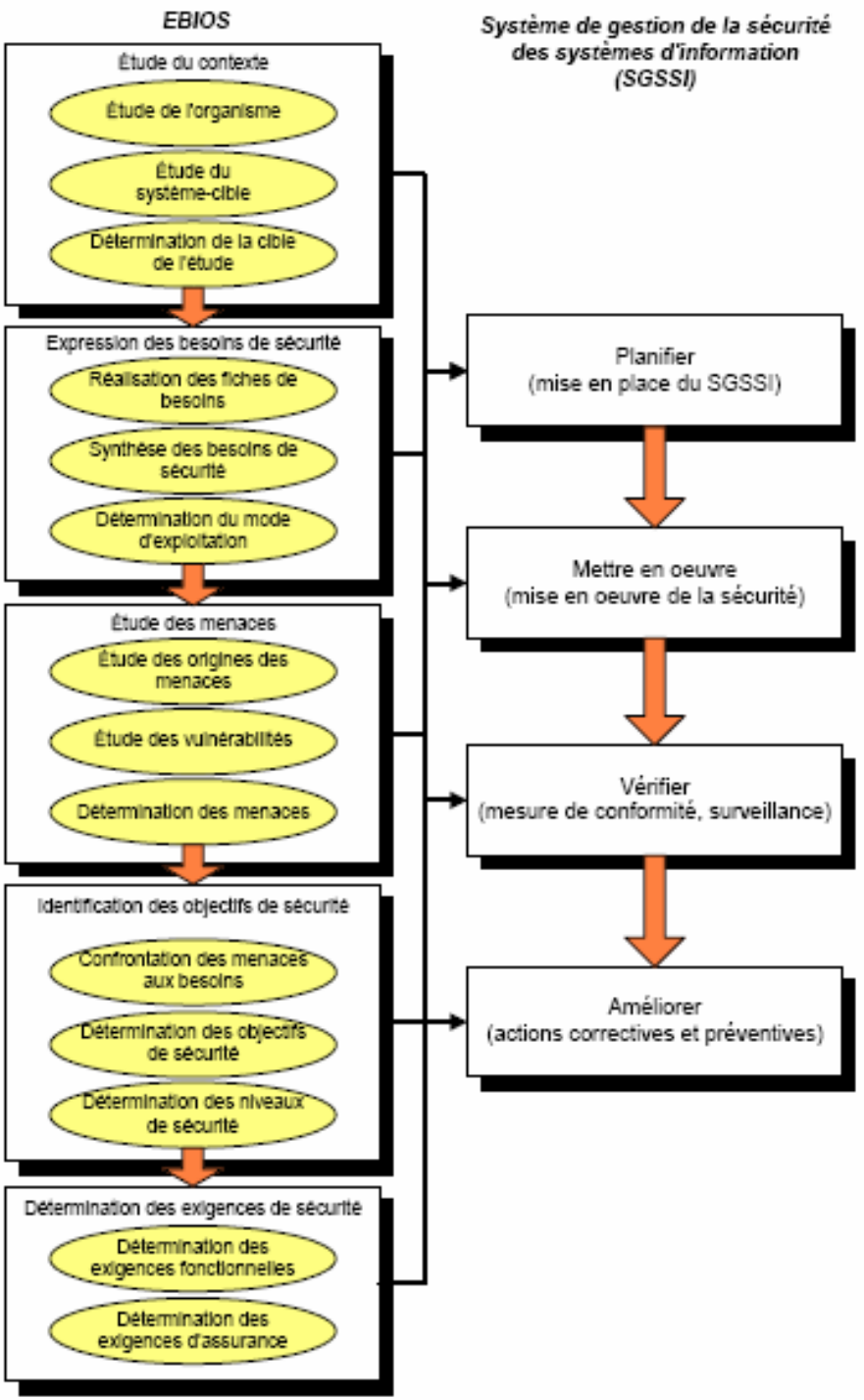
- Pour chaque mesure suggérée, considérez:
  - Alignement stratégique
  - Amélioration continuelle
  - Exigences légales
  - Avantages généraux
  - Economie (en temps et argent)
  - Réduction du risque
- et attribuez des priorités

- Planifiez – Implémentez – Contrôlez – Améliorez

EBIOS

(Expression des Besoins et Identification des Objectifs de Sécurité)

Français
DCSSI
Public
Complet

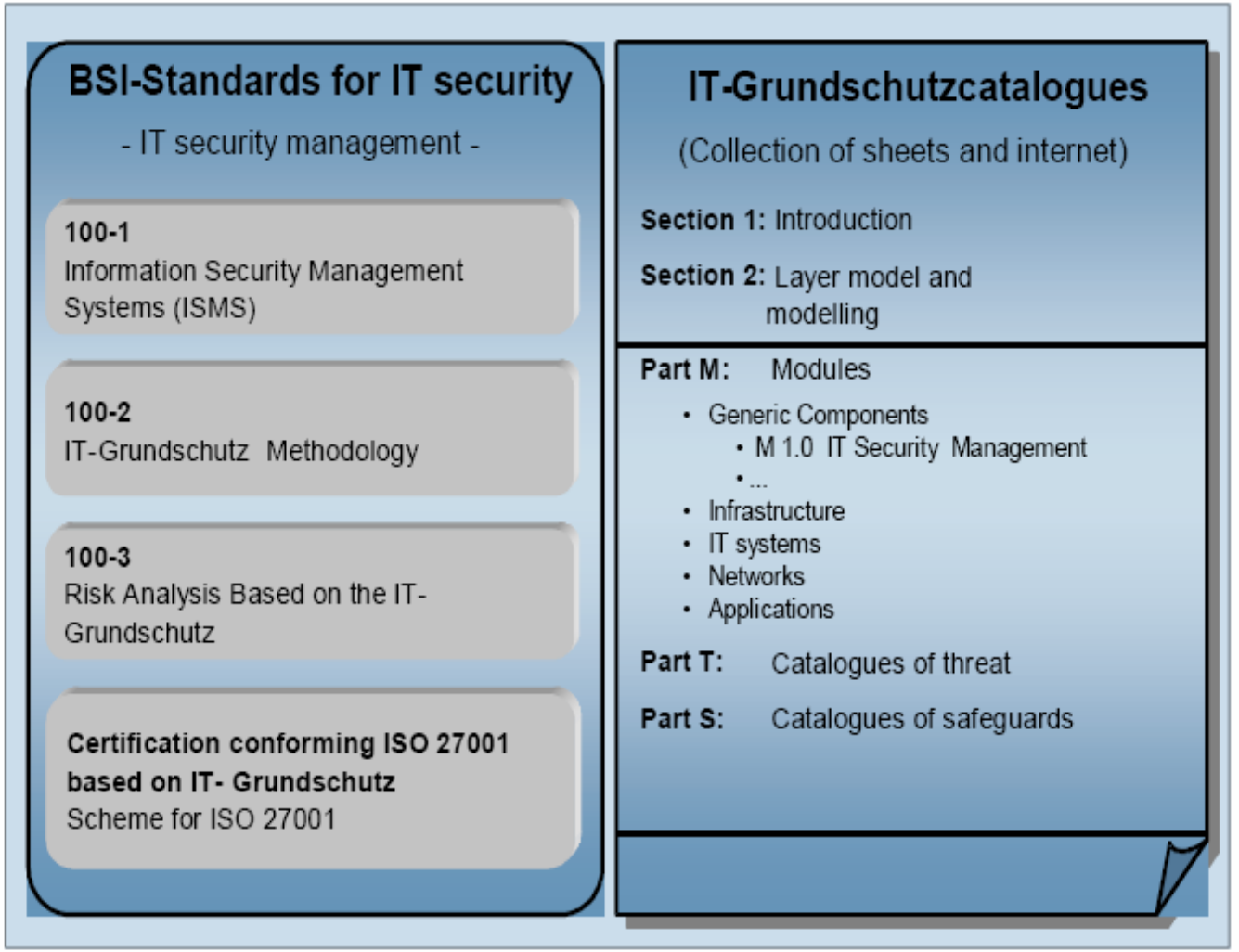


BSI Grundschutz

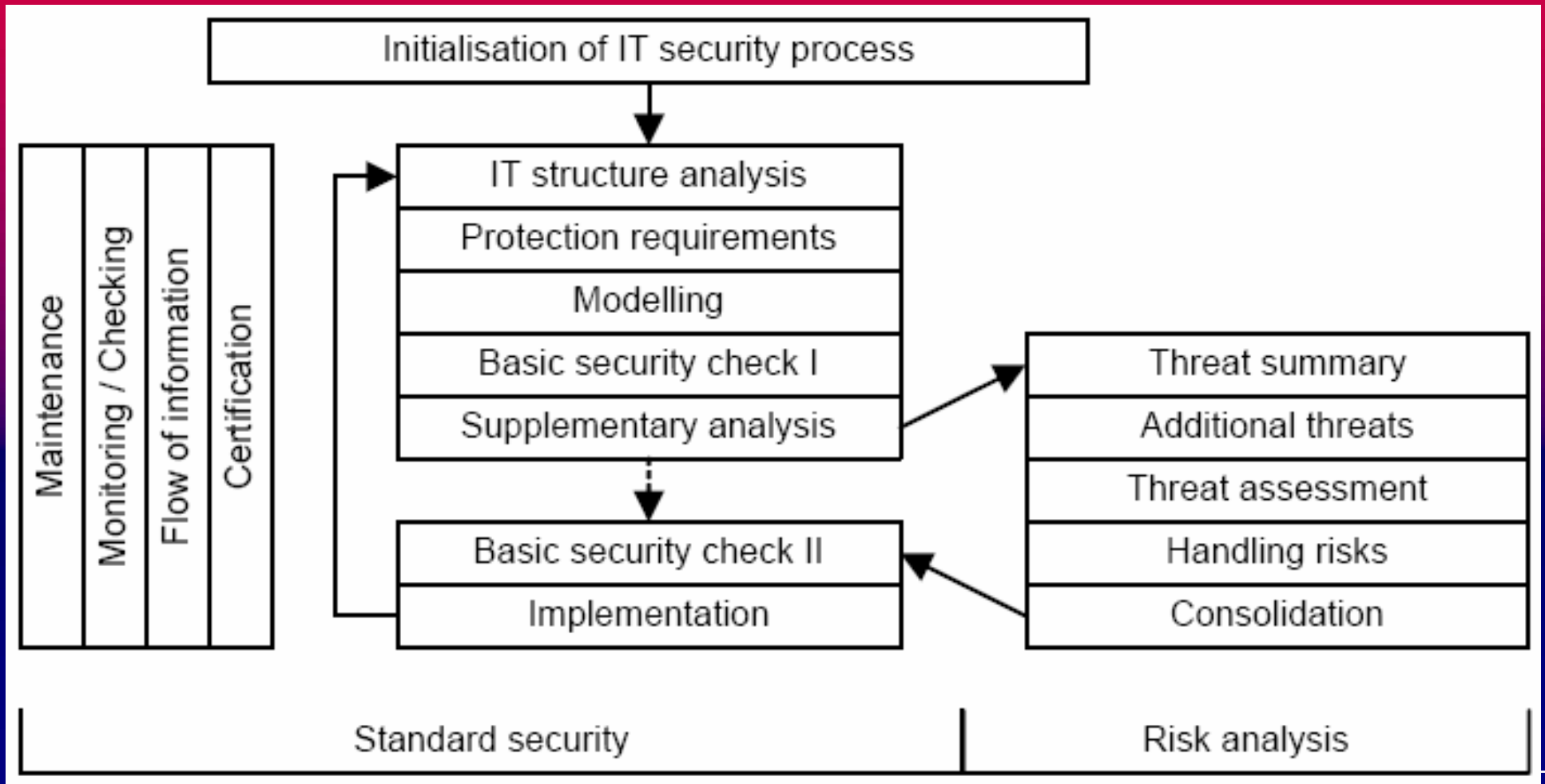
Bundesamt für Sicherheit in der Informationstechnologie

Guide d'implémentation ISMS
autour du C.I.D.
Accent sur l'élémentaire

- Inondation
- Update raté
- Personnel malade
- Marquage de confidentialité oublié



BSI Grundschutz



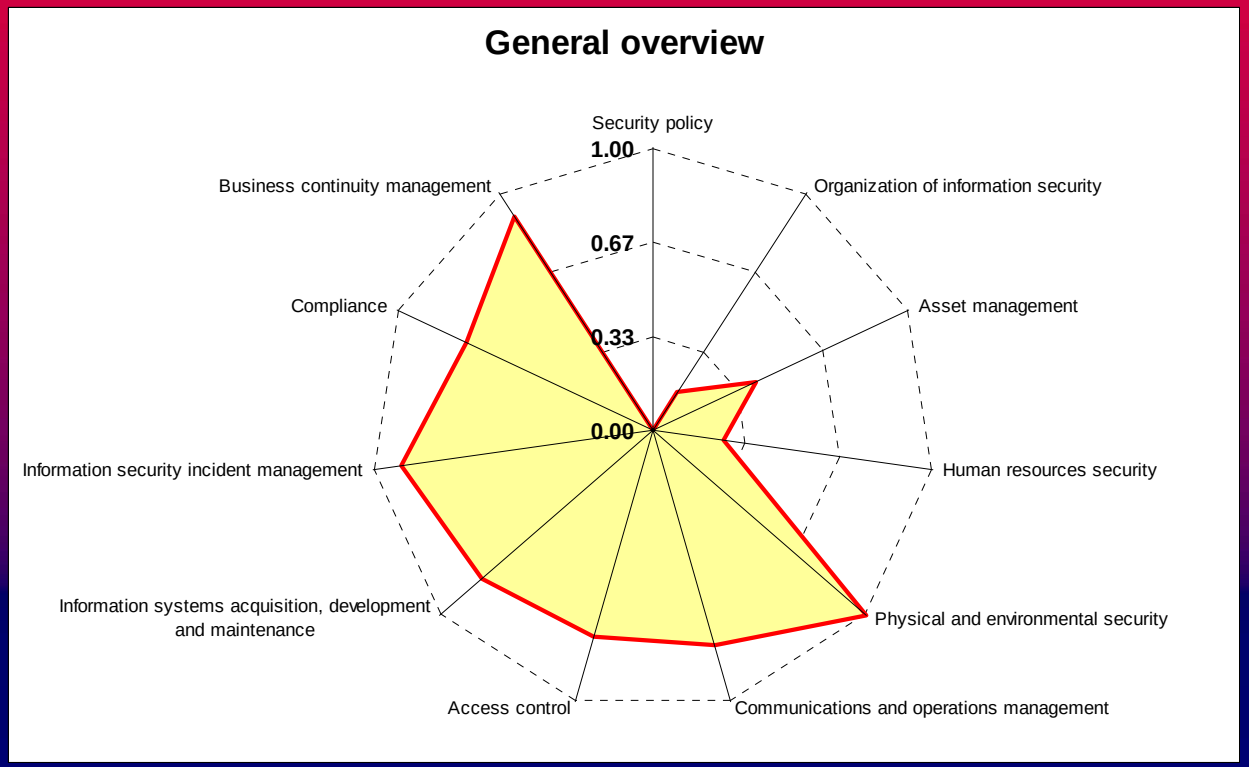
ISMS Certification

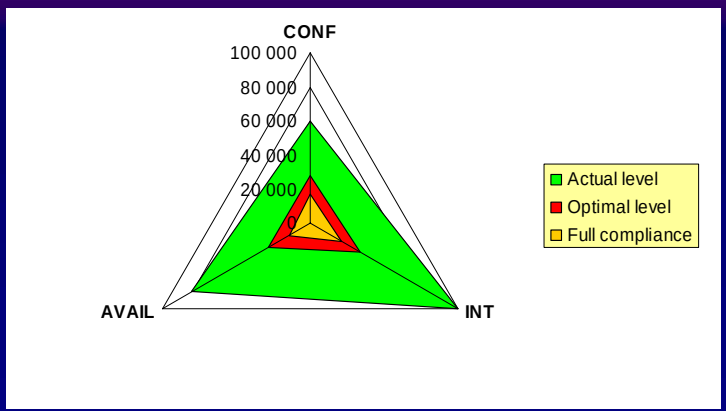
La certification ISMS selon ISO 27001 inclut une analyse de risques et tous les processus de gestion de la sécurité

Approche pragmatique: En x étapes, 2x le tour du PDCA

1. Périmètre et Politiques de sécurité haut niveau
2. Commencer avec une Analyse de Risques « Quick & Dirty »
3. Valeur de vos informations – Estimation ALE
4. Audit ISO 27002 – Coûts des mesures pertinentes
5. Implémentation des mesures les plus rentables
6. Implication du Management
7. Sensibilisation du personnel
8. …

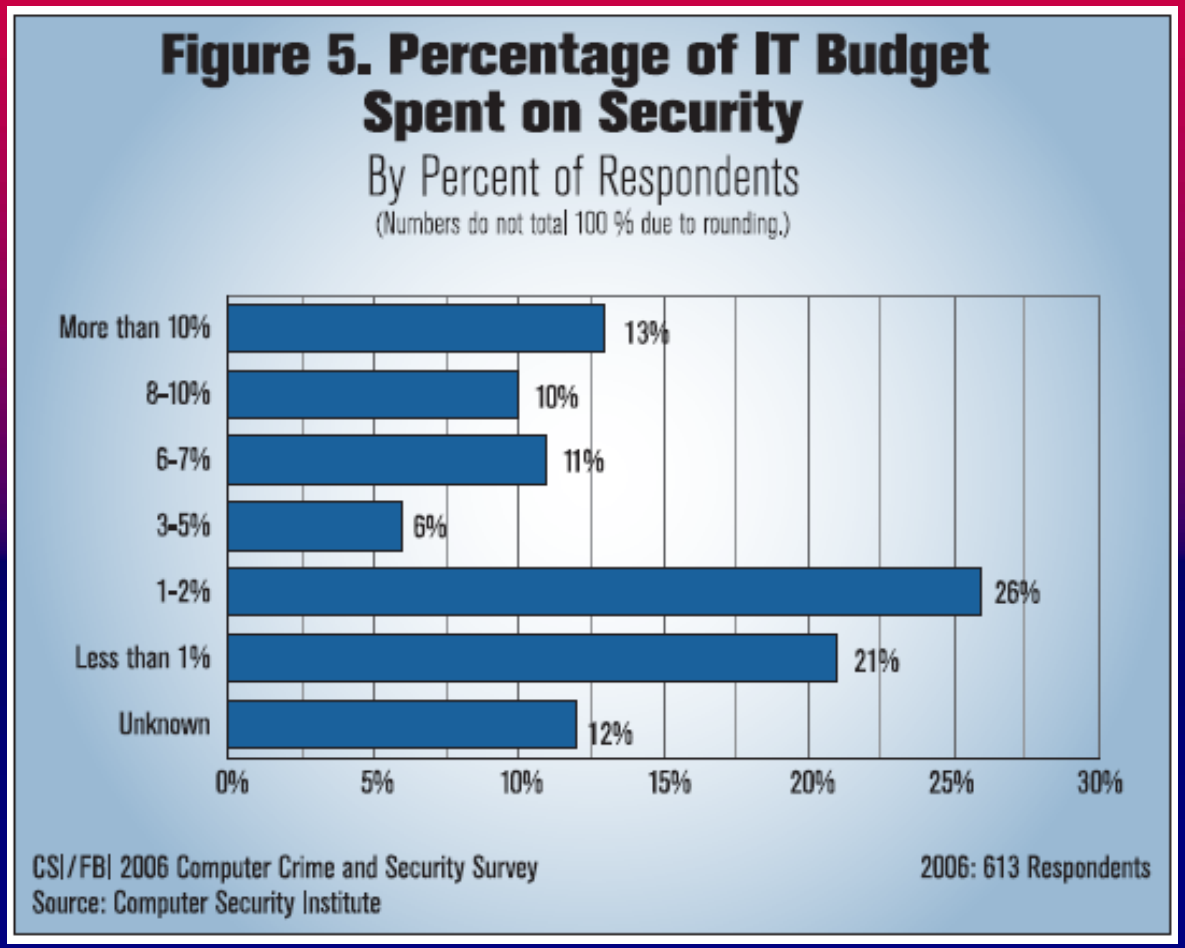
ISMS Certification





Source:Telindus

Dépense pour sécurité



Conclusion

Etablissez la valeur de vos informations

Démarrez une analyse de risques afin

- d'assurer l'efficacité de la sécurité en mettant les coûts en relation avec la réduction du risque obtenu
- d'anticiper les incidents (Gouverner c'est prévoir!)
- d'accepter des risques de façon consciente

Utilisez une méthode pragmatique

- qui convient à votre profil de risques
- qui établit vite une culture de gestion de risques et engendre une valeur ajoutée, plutôt que de viser une certification rapide.

Questions ?

Merci pour votre attention !

Carlo Harpes
harpes@vox.lu