BCP/DRP : méthodologies, processus & normes

ardantic SA

Jeff Primus & Henri Haenni

Senior Consultants

ISO27001 LA, ISO20000 LA, CISA CISSP, CRISC, CGEIT, AMBCI

bienvenue@ardantic.ch

A propos dôardantic

- **Services** de consultance, de formation et dôaudit
  - ✓ Gouvernance IT et Sécurité
- **Mission**:
  - ✓ création de valeur et diminution du risque pour les entreprises
- **Consultants Seniors**
  - ✓ (EPFL, MBA) actifs depuis une vingtaine dôannée
- **Certifications**:
  - ✓ CISSP, CISA, CRISC, CGEIT, AMBCI, ISO 27001 LA, ISO 20000 LA
- **Indépendant** des fournisseurs
- **Basée** à Pully - Vaud

Services dôardantic : création de valeur

- Alignement Métier & IT, planification stratégique
- Tableaux de bord, KPI & KRI
- Modélisation de catalogues de services
- Processus IT
- Implémentation de ISO 20000
- Architecture et urbanisation de SI
- Formation, certification
- Gestion de projet
- Assistance MOA
- Sourcing et gestion contractuelle

Services dôardantic : réduction du risque

- Stratégie sécuritaire, programme de sécurité
- Tableaux de bord de la sécurité des SI
- Architectures sécuritaires
- Implémentation de ISO 27001/27002
- Plan de continuité opérationnelle
- Plan de reprise en cas de désastre
- Plans pandémie
- Sensibilisation à la sécurité
- Formation

Services dôardantic : évaluation

- Audits IT & de sécurité
- Analyses de risques
- Audits Single Point of Failure
- Évaluation de conformité
  - COBIT, ITIL, ISO 20000 & 27001 & 27005
  - Basel II, SOX, IFRS
- Évaluation de sécurité partenaires

Formations

- **ISEIG ï Formations :**
  - ISO 27001 / 27002 / 27005
  - CISA
  - Gestion de Risques
  - Brevet Fédéral dôinformaticien
- **HEIG-VD:**
  - Chargé de cours Sécurité des systèmes dôinformation
- **Paris ï Sorbonne**
  - Chargé de cours - Gouvernance et Sécurité SOA

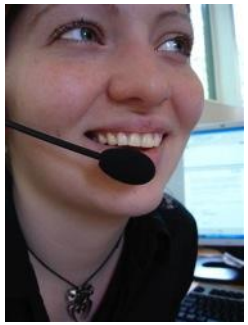
Missions

- **Grandes administrations publiques:**
  - Audits de sécurité
  - Plans de continuité
  - Politiques de sécurité organisationnelles et techniques
- **Organisations internationales et locales :**
  - Analyse des risques de la sécurité de lôinformation
  - Audits selon ISO 20000 et ISO 27001
  - Mise en conformité PCI
  - Analyse des risques opérationnels
- **Industries :**
  - Assistance MOA
  - Conduite dôappels dôoffres
  - Structurations organisationnelles
  - Programme de sécurité

Agenda

SECTION 1 – PLANIFIER l'INPLANIFIABLE

Quand tout va bienéé

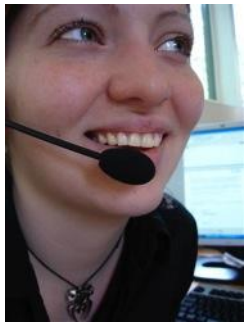


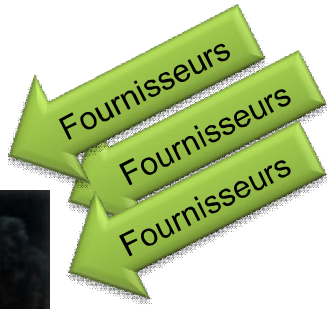
Commandes

Fournisseurs

Livraisons

Mais si tout va malé





Vulnérabilités : Organisations intégrées

Banques

Assurances

Distributeurs

Autorités

Fournisseurs

Clients

RH

Infrastructures

Bureaux

Datacenter

Transports

Finances

Personne nôest à lôabri

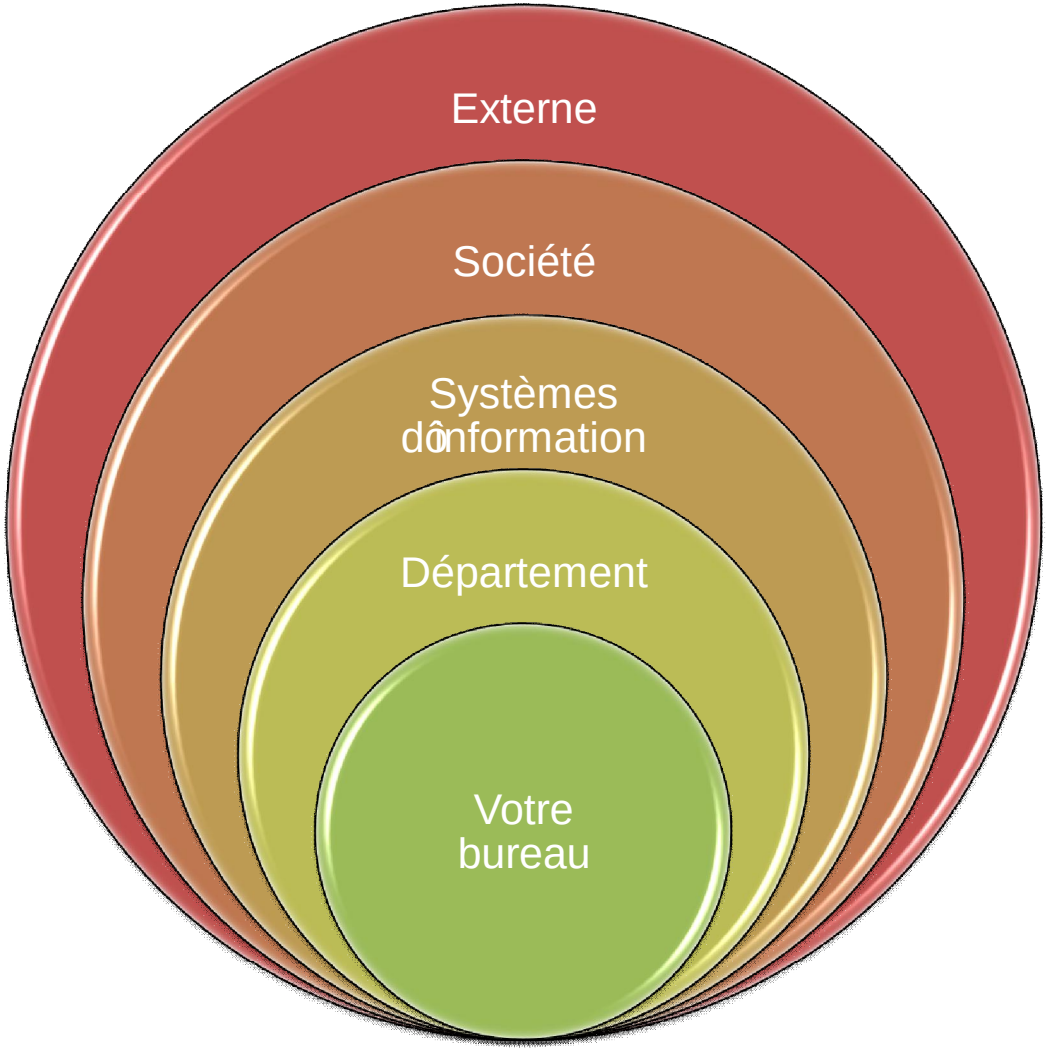
La catastrophe
est liée à
lôactivité humaine

- Impossibilité de tout prévoir
- Systèmes trop complexes et/ou trop vulnérables
- Multiplicité des effets de bord
- Entropie naturelle
- Prise de risques
- Allocation des priorités
- Sous-estimation des dangers
- Ignorance

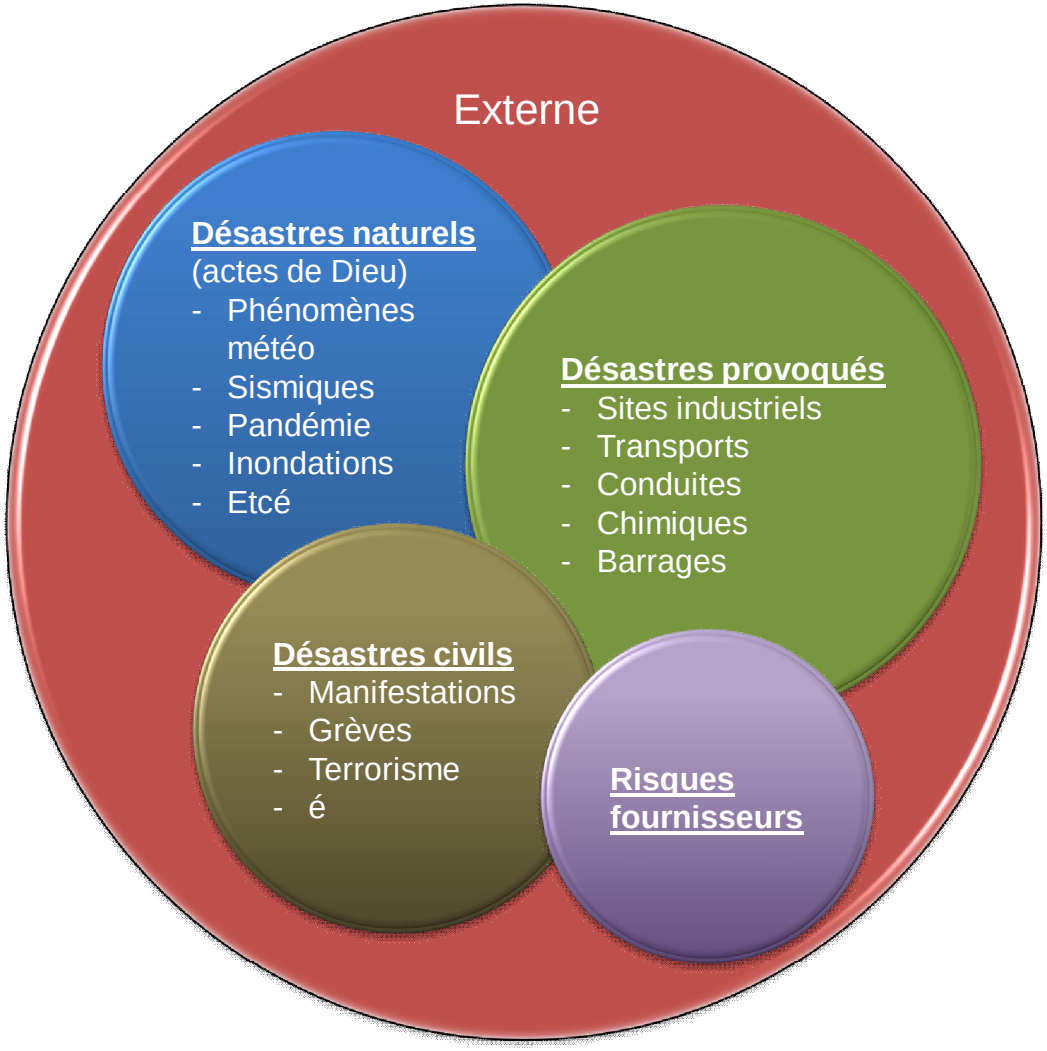
INEVITABILITE

PREPARATION

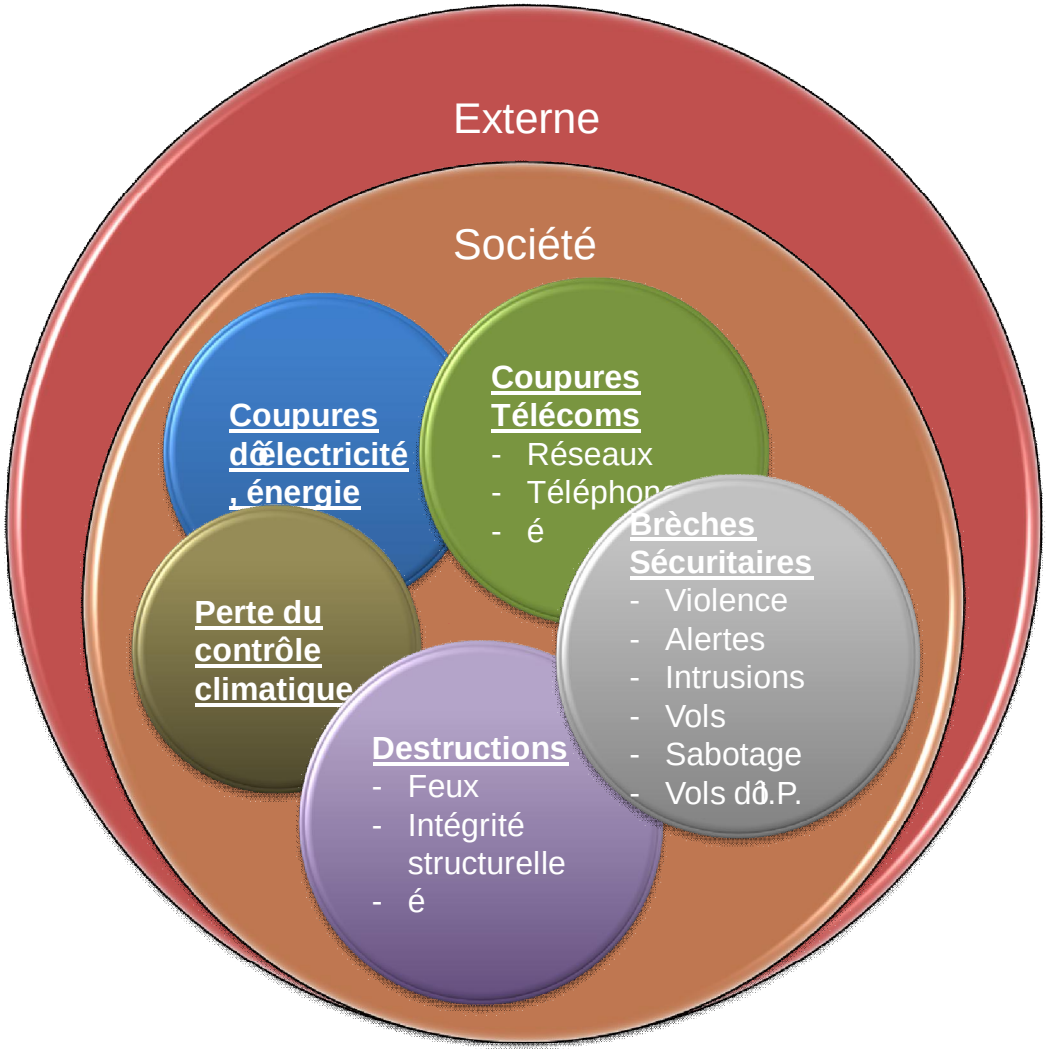
Taxonomie des sinistres et désastres
Portée



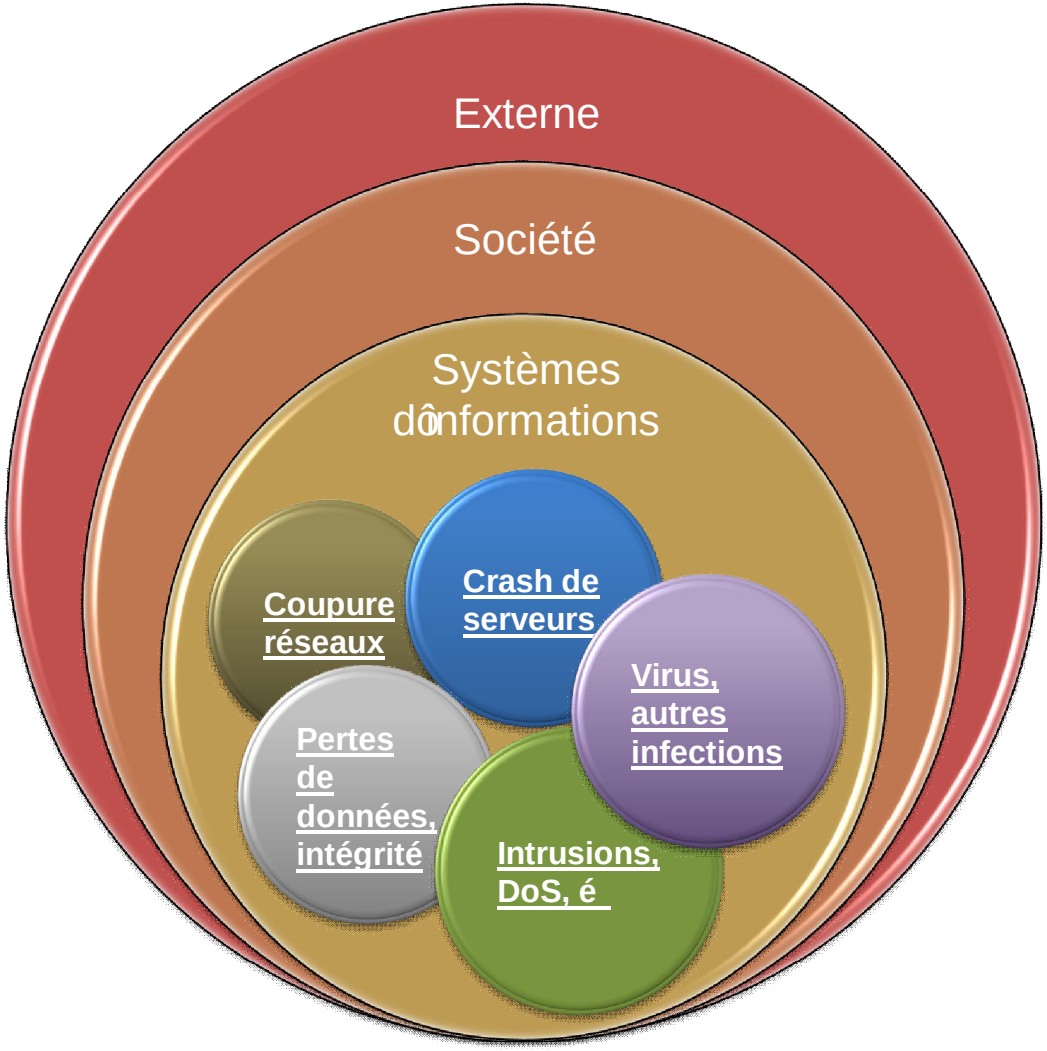
Taxonomie des sinistres et désastres
Portée - externe



Taxonomie des sinistres et désastres
Portée - société



Taxonomie des sinistres et désastres
Portée ï systèmes dônformation



Dommages et conséquences
Temporalité

Département ou systèmes d'information

Société

Ecosystème de la société

Impacts directs

- *Indisponibilités*
- *Pertes d'informations*
- *Destructions*

Impacts indirects

- Retards de livraison
- Délais non respectés
- Surcharges opérationnelles
- Erreurs
- Perturbations logistiques

Effets à long terme

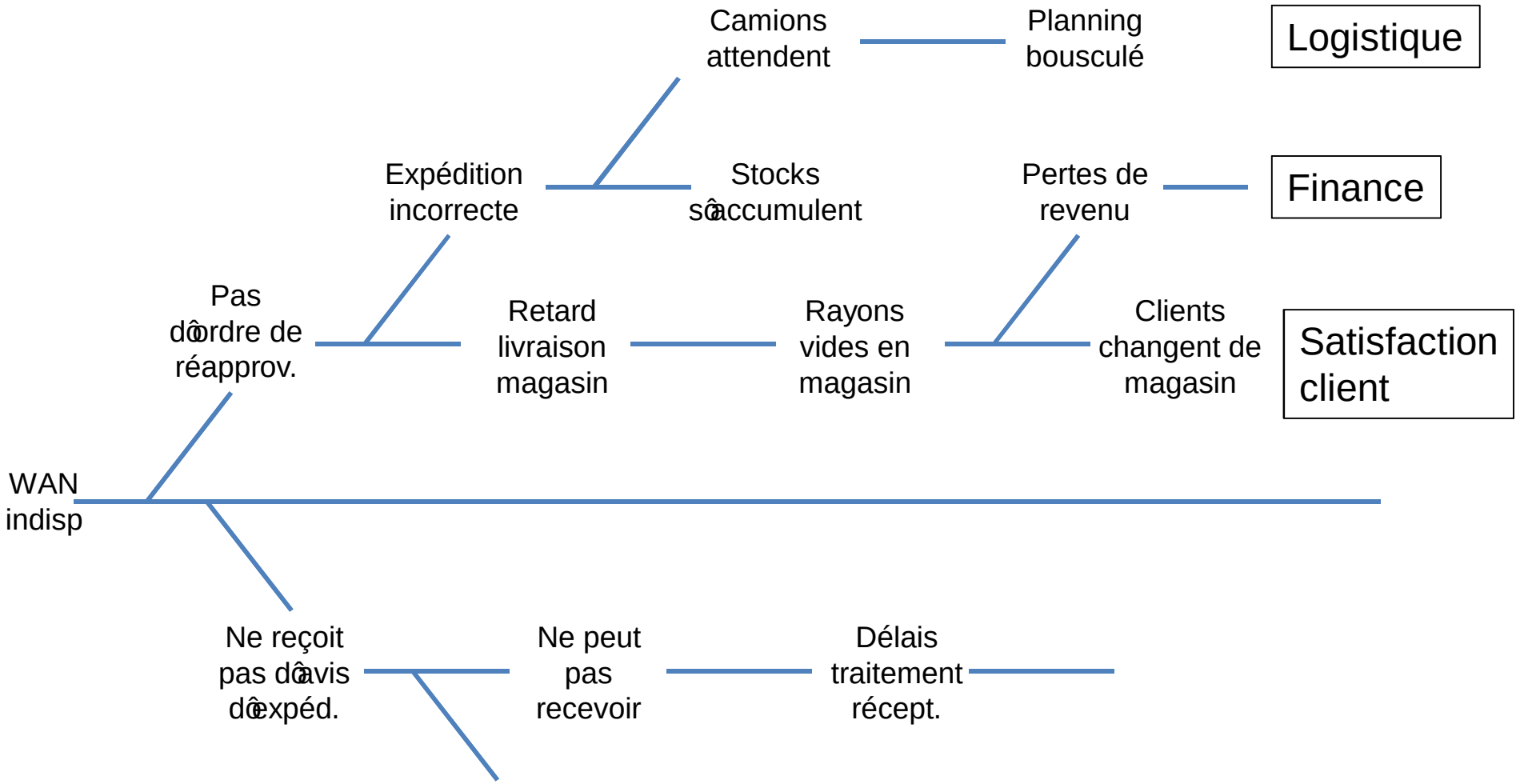
- Atteintes à l'image
- Pertes de parts de marché
- Pertes de confiance (clients, investisseurs)
- Plaintes, procès, …
- Image publique érodée

$

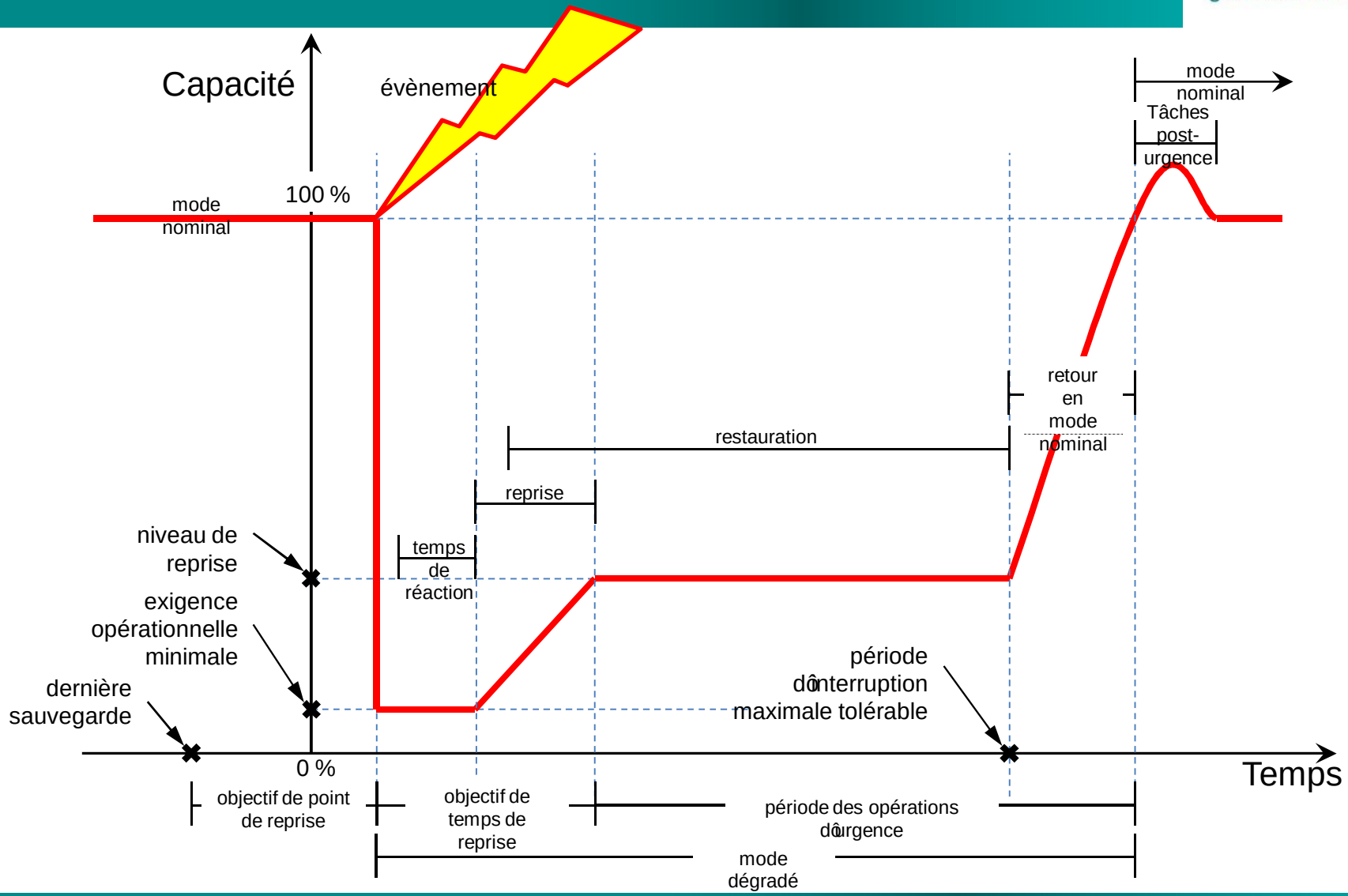
$$

$$$

Dommages et conséquences
Diagramme d'effet (exemple)



Anatomie dûne situation de continuité




SECTION 2 – DEVELOPPER
LA RESILIENCE

Objectif de la résilience

re·sil·ience
n.
1. The ability to recover quickly from illness, change, or misfortune; buoyancy.
2. The property of a material that enables it to resume its original shape or position after being bent, stretched, or compressed; elasticity.

Assurer que les processus métiers critiques sont disponibles pour tous les tiers devant avoir accès à ces fonctions

La résilience est donc l'ensemble des programmes, directives, procédures et standards utilisés pour qu'une organisation continue ses activités, quelques soient les circonstances ou les évènements adverses survenant.

Assurer la continuité est une activité quotidienne, intégrée à la culture de l'organisation

Cadre de la résilience et de la continuité

Places de travail

Personnel

Syst. d'information

Infrastructure

Information

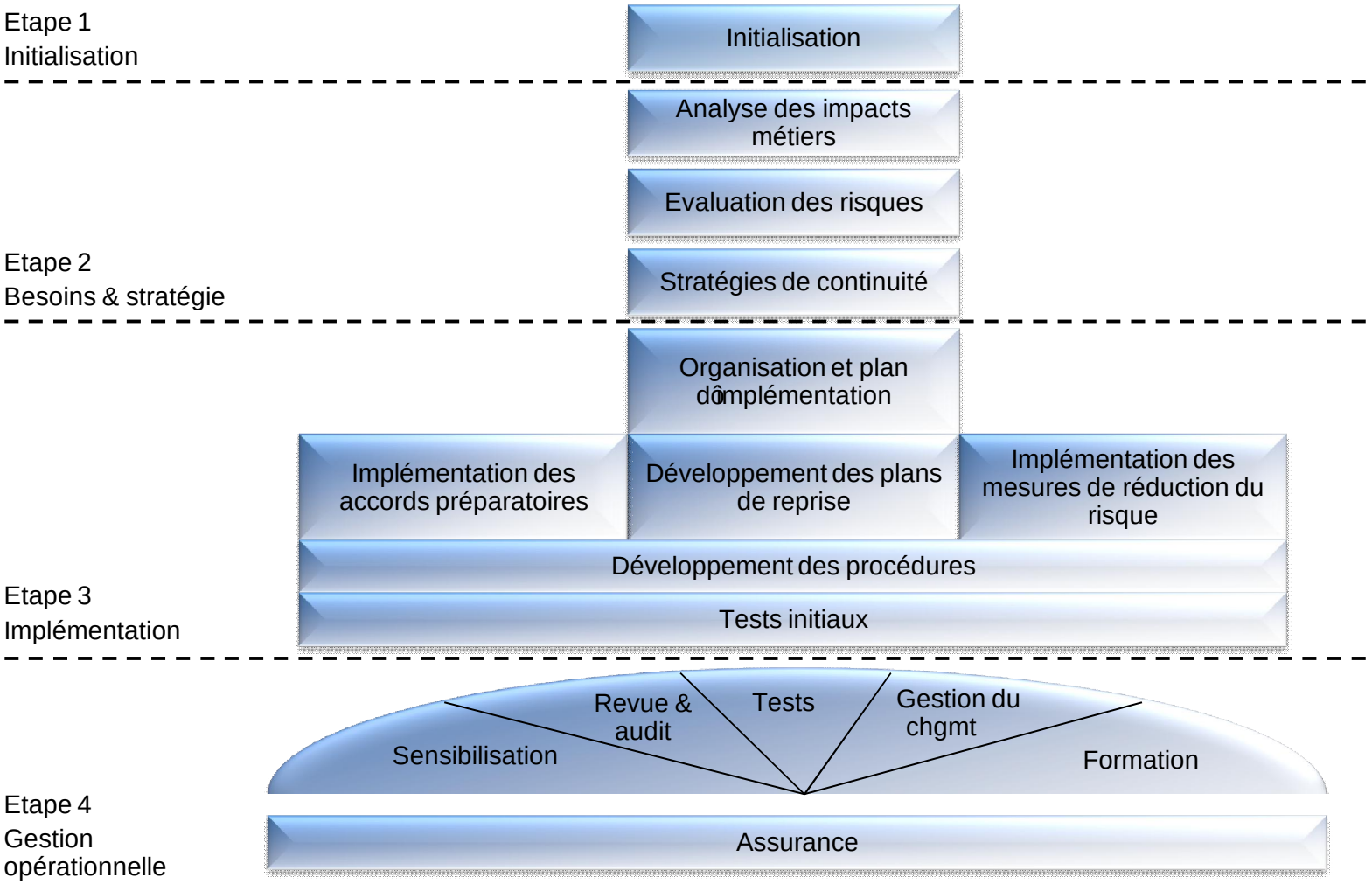
Fournisseurs

Les capacités internes de l'entreprises

Des partenariats coopératifs

Des solutions commerciales

Processus général



Processus général : initialisation

Etape 1
Initialisation

Initialisation

- Définition du cadre de la continuité
- Rédaction de la politique de continuité
- Établissement du processus de continuité
- Compréhension de l'organisation
- Allocation des responsabilités (organisation du projet)
- Soutien du management (sponsorship)
- Obtention du budget
- Identification des ressources

Enoncé de cadre

Politique de continuité (déclaration d'intention)

Charte du projet de continuité

Processus général : besoins et stratégies

Analyse des impacts métiers

Evaluation des risques

Stratégies de continuité

Etape 2
Besoins & stratégies

Répondre à 2 questions :

Comment l'organisation survivra t-elle à un désastre ou une interruption des affaires ?

Quels sont les coûts et les conséquences liés à un désastre ou une interruption des affaires ?

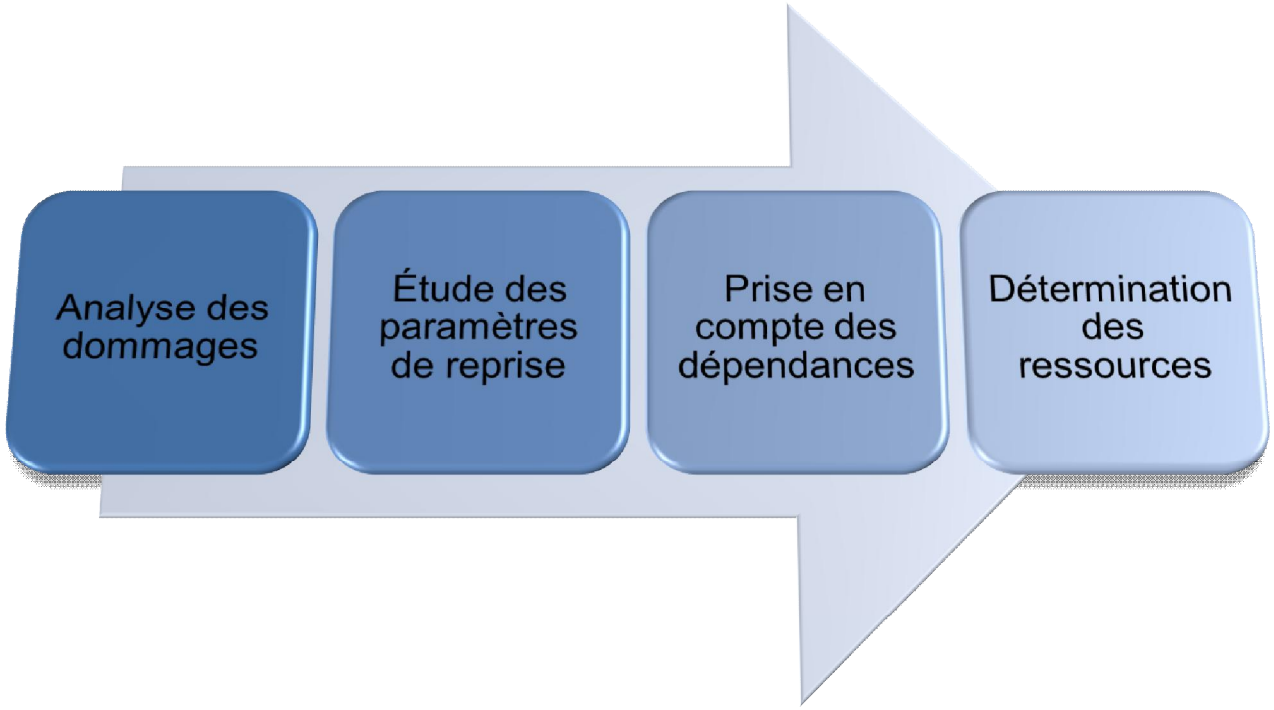
Processus général : besoins et stratégies

Analyse des impacts métiers

Evaluation des risques

Stratégies de continuité

Etape 2
Besoins & stratégies



Rapport d'analyse des impacts métiers

Processus général : besoins et stratégies

Analyse des impacts métiers

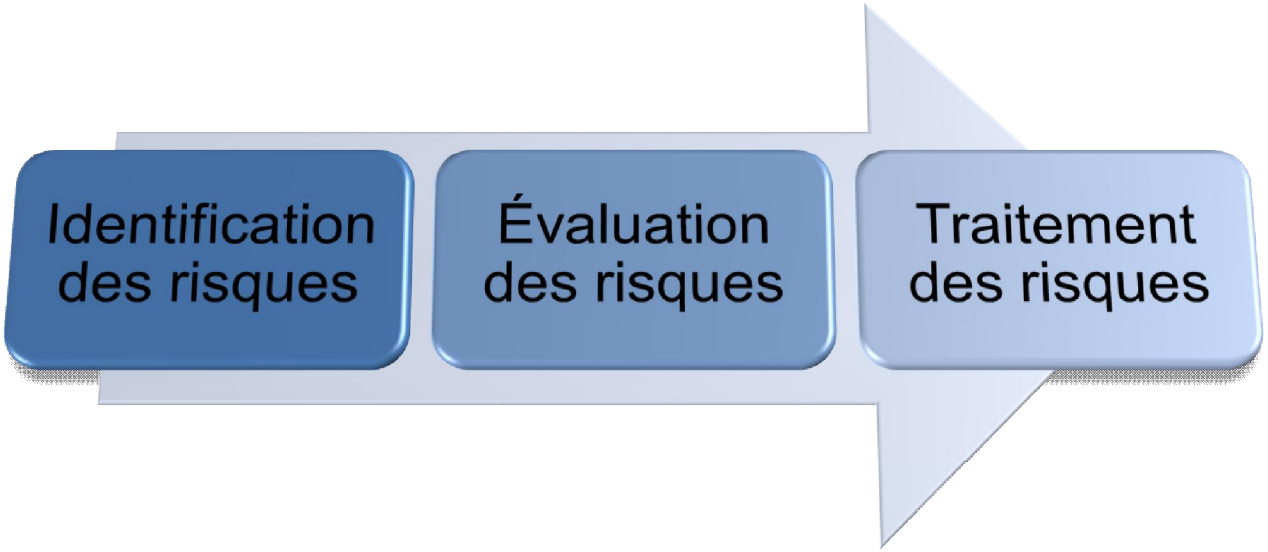
Evaluation des risques

Stratégies de continuité

Etape 2
Besoins & stratégies

Objectifs :

- Rendre les risques clairs pour les décisionnaires
- Développer des contremesures pour réduire ces risques
- Identifier les scénarios pour lesquels des plans de continuité doivent être testés



Rapport d'analyse des risques

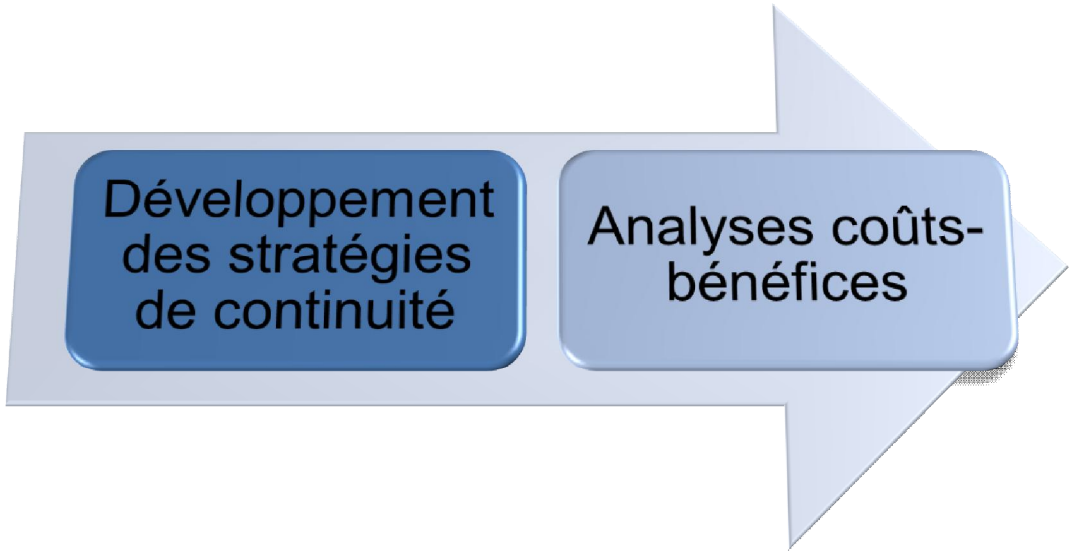
Processus général : besoins et stratégies

Analyse des impacts métiers

Evaluation des risques

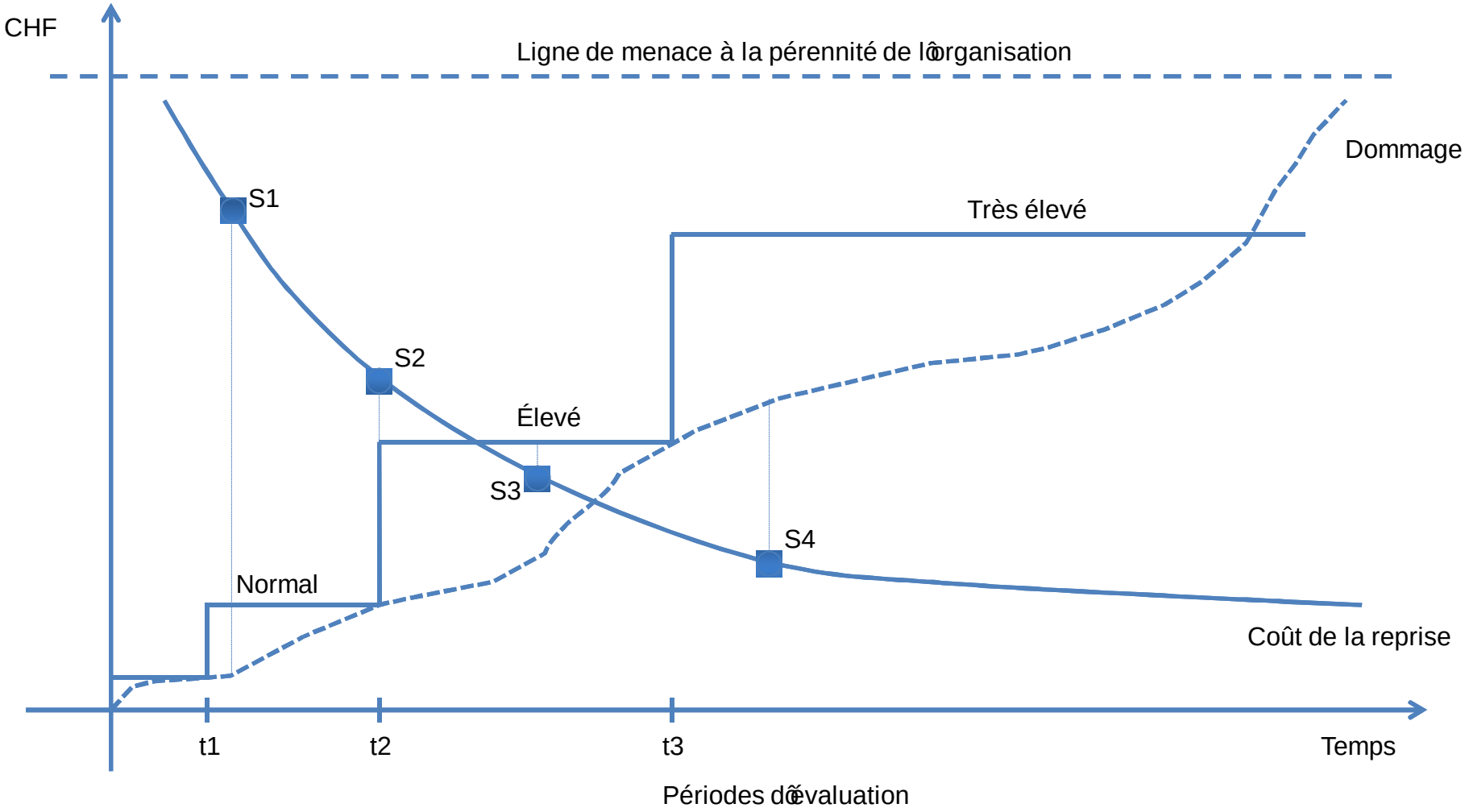
Stratégies de continuité

Etape 2
Besoins & stratégies

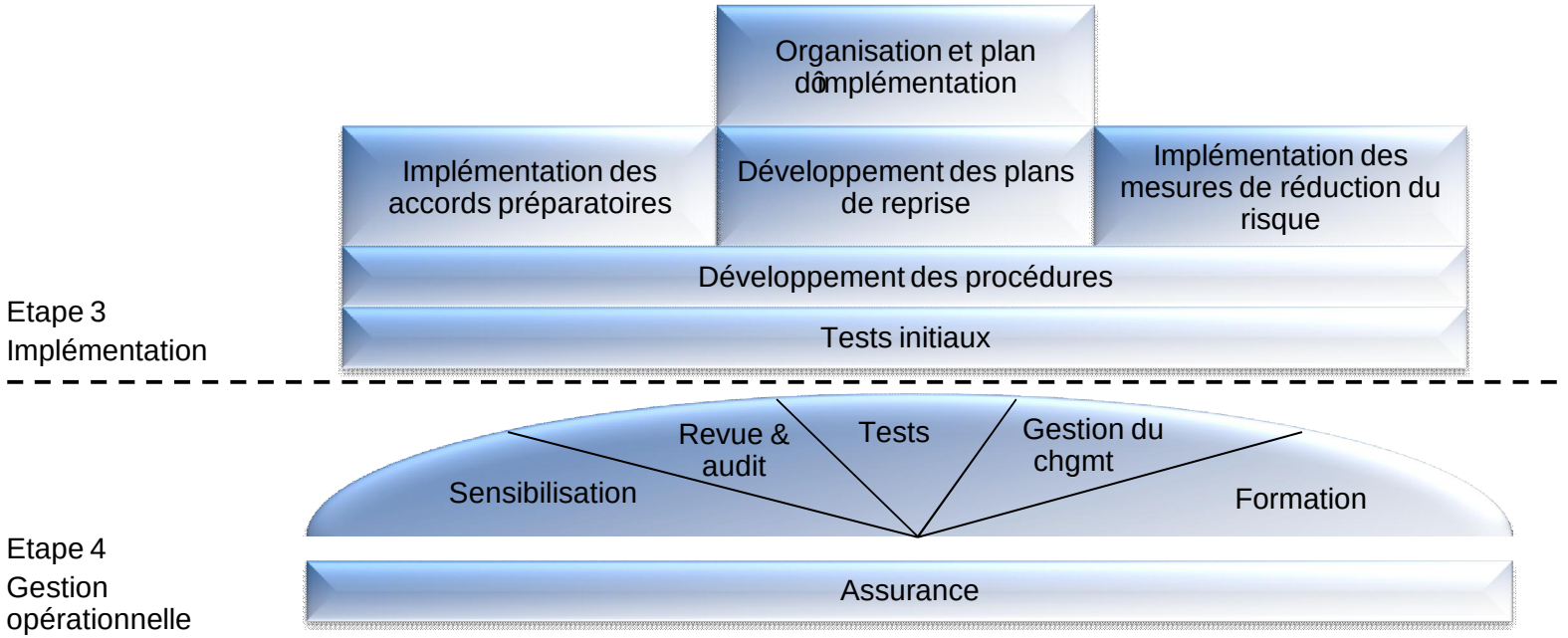


Stratégies de continuité

Processus général : besoins et stratégies



Processus général : implémentation et gestion opérationnelle



Gestion de la continuité
Les 10 commandements

1. **LE PILOTAGE DE LA CONTINUITÉ AU BUSINESS TU CONFIERAS**
   - ✓ *L'IT n'est qu'un des volets de la continuité à adresser*
2. **LA CONTINUITÉ AUX ACTIVITÉS QUOTIDIENNES DE L'ENTREPRISE TU INTÈGRERAS**
   - ✓ *Les plans de continuité doivent être le reflet de l'activité au quotidien*
3. **AUX NORMES SEULEMENT DE TE BASER TU ÉVITERAS**
   - ✓ *Les normes et standards sont des guides, souvent très génériques; il convient de multiplier les sources d'information et de se faire aider*
4. **LA CONTINUITÉ, COMME UN OUTIL DE GOUVERNANCE TU CONSIDÈRERAS**
   - ✓ *La gestion de la continuité n'est pas qu'un outil de sécurité mais doit être vue comme un moyen de gagner en visibilité sur ce que le business fait réellement, comment il le fait et de quoi il a besoin*

Gestion de la continuité
Les 10 commandements

5. **SUR LES SCÉNARIOS DE DÉSASTRE SEULEMENT, TES PLANS TU NE BASERAS**
   - ✓ *Le développement des plans doit être holistique, méthodologique et systématique; les scénarios sont utilisés pour tester des plans existants*
6. **CONCIS ET JUDICIEUSEMENT ORGANISÉS, TES PLANS TU MAINTIENDRAS**
   - ✓ *Les documents doivent être aisément lisibles en cas de crise; on les maintiendras simples, précis, sans renvois, analyses de fonds ou références historiques*
7. **SUR UNE PLATEFORME FACILEMENT ACCESSIBLE, TES PLANS TU GARDERAS**
   - ✓ *Les plans doivent être d'accès rapide (intranet) et des copies papier seront produites et conservées hors des locaux*

Gestion de la continuité
Les 10 commandements

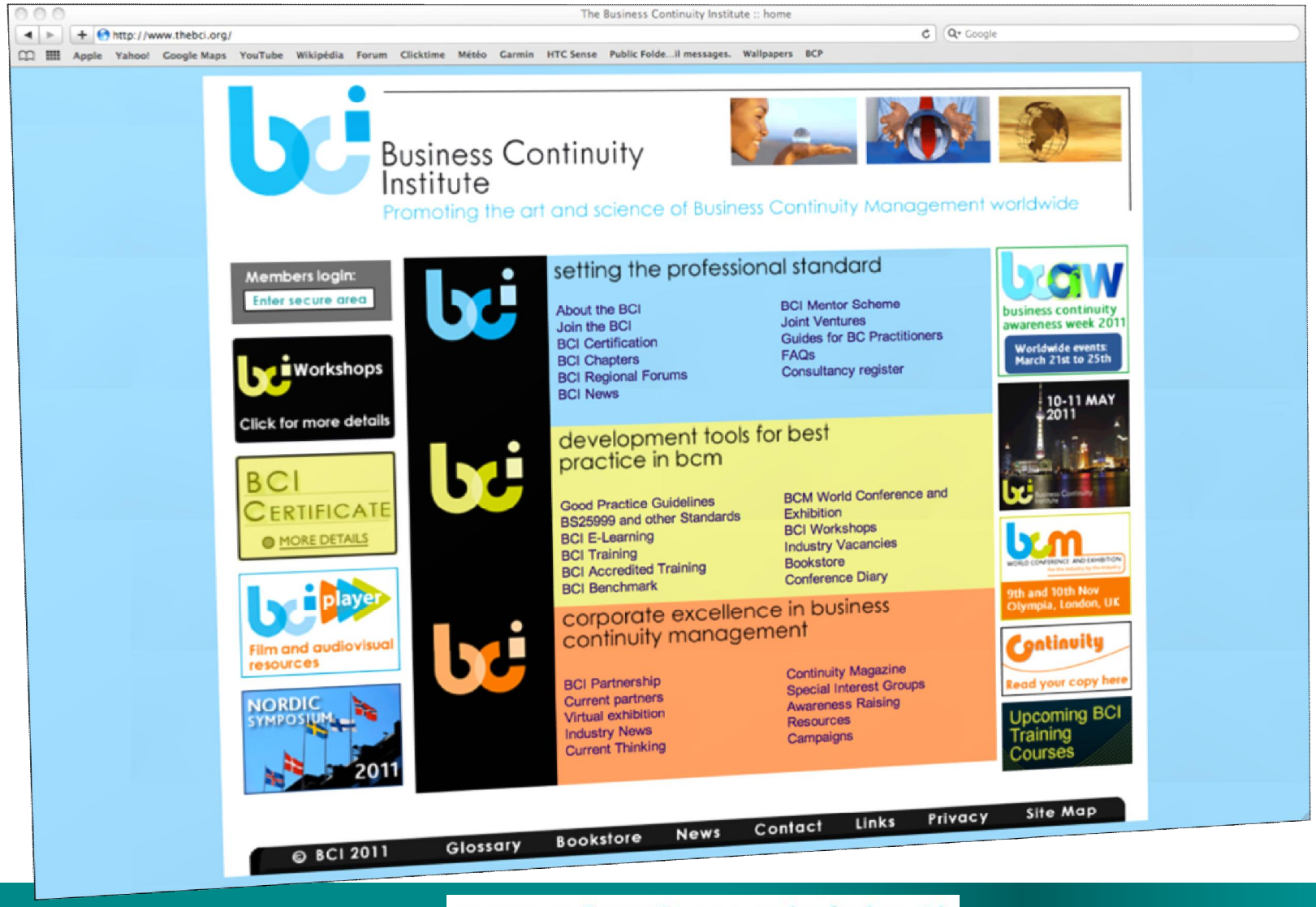
8. **LES CONSULTANTS AUX APPROCHES « CLÉ-EN-MAIN » TU TE MEFIERAS**
   - ✓ *La continuité est un processus d'apprentissage, on préfèrera donc l'approche méthodologie-centrique assortie d'un coaching assurant la pérennité des investissements*
9. **UN LOGICIEL DE GESTION DE LA CONTINUITÉ TU UTILISERAS**
   - ✓ *La gestion de la continuité produit un volume tout de même important de documentation; un logiciel spécialisé est très fortement recommandé*
10. **LES VENDEURS SANS MÉTHODOLOGIE INDÉPENDANTE TU ÉVITERAS**
    - ✓ *Afin de ne pas adapter les besoins de votre entreprise aux exigences des consultants et de leur logiciel*


SECTION 3 – CENTRES DE RESSOURCES & REFERENTIELS NORMATIFS

Quelques standards et normes dans le monde

	NFPA 1600 (2007) : Standard on Disaster/Emergency management and Business Continuity Programs NIST SP800-34 (2002) : Contingency planning guide for information technology systems
	AS HB 292-2006 : A practitioners guide to business continuity management AS HB 293-2006 : Executive guide to business continuity management AS/NZ 5050:2010 : Business continuity ï manging disruption-related risks
	BS 25999-1 (2006) : Business Continuity management, Code of Practice, BS 25999-2 (2007) : Specification for Business Continuity Management, BS 25777 (2008) : Information and communication technology continuity management, Code of Practice
	AFNOR BP Z74-700 : plan de continuité dâactivité (PCA)
	BSI ï IT Grundschutz 100-4 : Business Continuity Management
	ANSI/ASIS SPC.1-2009 Organizational Resilience ï Security, Preparedness & Continuity Management Systems
	ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management

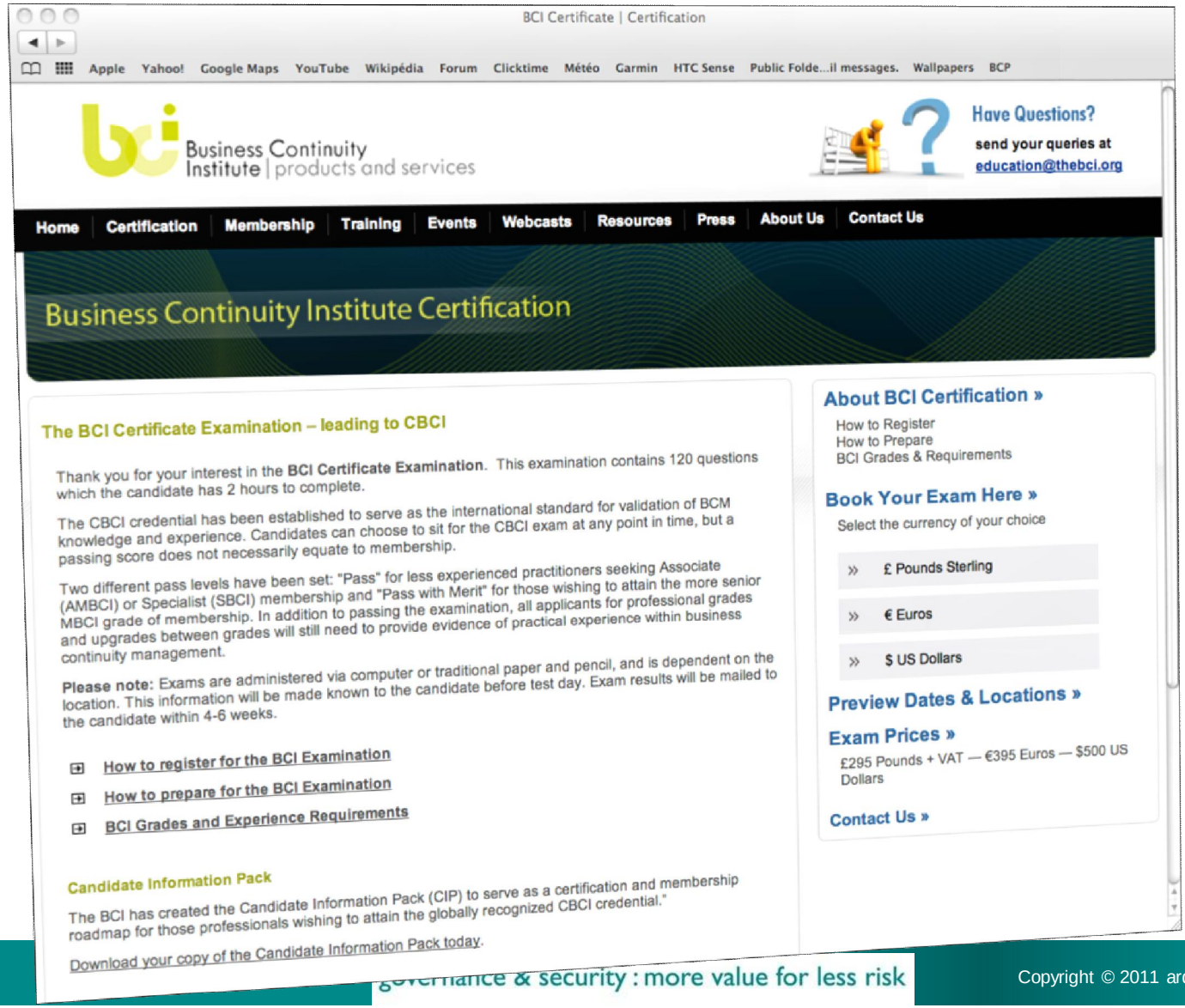
The Business Continuity Institute



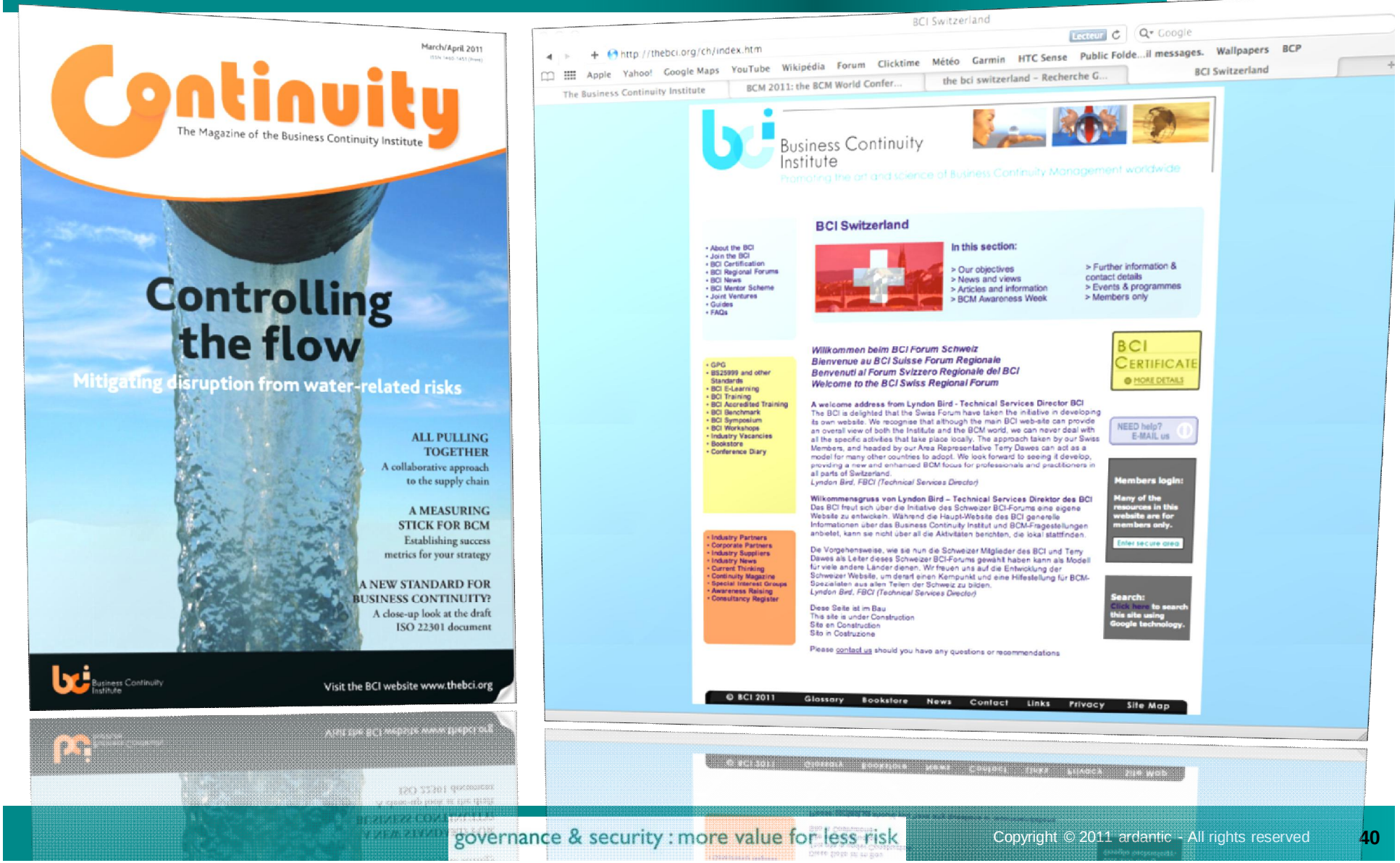
The Business Continuity Institute : Ressources

Good Practices Guidelines 2010 :

The Business Continuity Institute : Schème de certification



The Business Continuity Institute : Publications et chapitres locaux



more value for less risk !

ardantic
governance & security

Merci pour votre attention !

Nous restons à votre disposition pour toute questions ou informations

Pour nous contacter :
info@ardantic.ch

Services dâardantic

more value for less risk !

ardantic
governance & security

Merci pour votre attention !

Nous restons à votre disposition pour toute questions ou informations

Pour nous contacter :
info@ardantic.ch