

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 d'ardantic



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

Services d'ardantic : 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 d'Ardantic : 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 d'ardantic : 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



- “ **ISEIG È Formations :**

- “ ISO 27001 / 27002 / 27005
- “ CISA
- “ Gestion de Risques
- “ Brevet Fédéral d'informaticien

- “ **HEIG-VD:**

- “ Chargé de cours Sécurité des systèmes d'information

- “ **Paris È 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 l'information
 - “ Audits selon ISO 20000 et ISO 27001
 - “ Mise en conformité PCI
 - “ Analyse des risques opérationnels
- “ **Industries :**
 - “ Assistance MOA
 - “ Conduite de appels d'offres
 - “ Structurations organisationnelles
 - “ Programme de sécurité



Agenda



LIVE

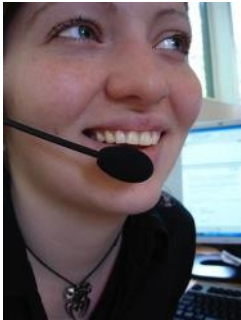
**SECTION 1 – PLANIFIER
L'INPLANIFIABLE**

BREAKING NEWS

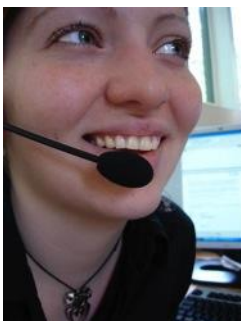
**Small aircraft crashes into
building near E. 72nd & York**



Quand tout va bienÅ



Mais si tout va malÅ

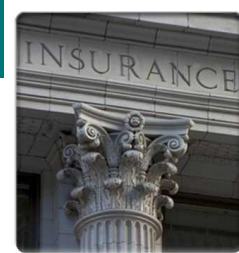


Vulnérabilités : Organisations intégrées

Distributeurs



Banques



Assurances



Autorités

Fournisseurs



Clients



RH



Infrastructures



Bureaux



Datacenter



Transports



Finances



Personne n'est à l'abri



La catastrophe
est liée à
l'activité humaine



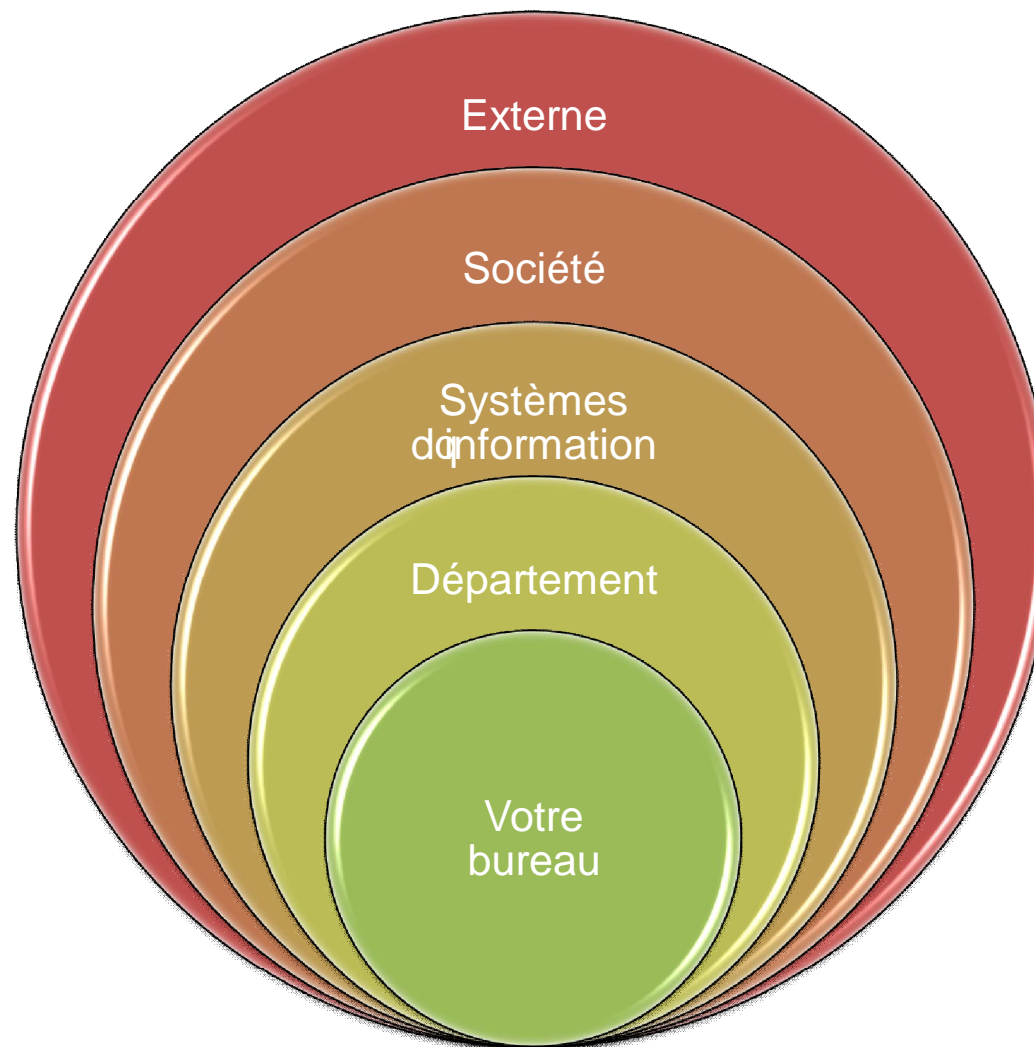
- “ Impossibilité de tout prévoir
- “ Systèmes trop complexes et/ou trop vulnérables
- “ Multiplicité des effets de bord
- “ Entropie naturelle
- “ Prise de risques
- “ Allocation des priorités
- “ Sous-estimation des dangers
- “ Ignorance



INEVITABILITE
PREPARATION

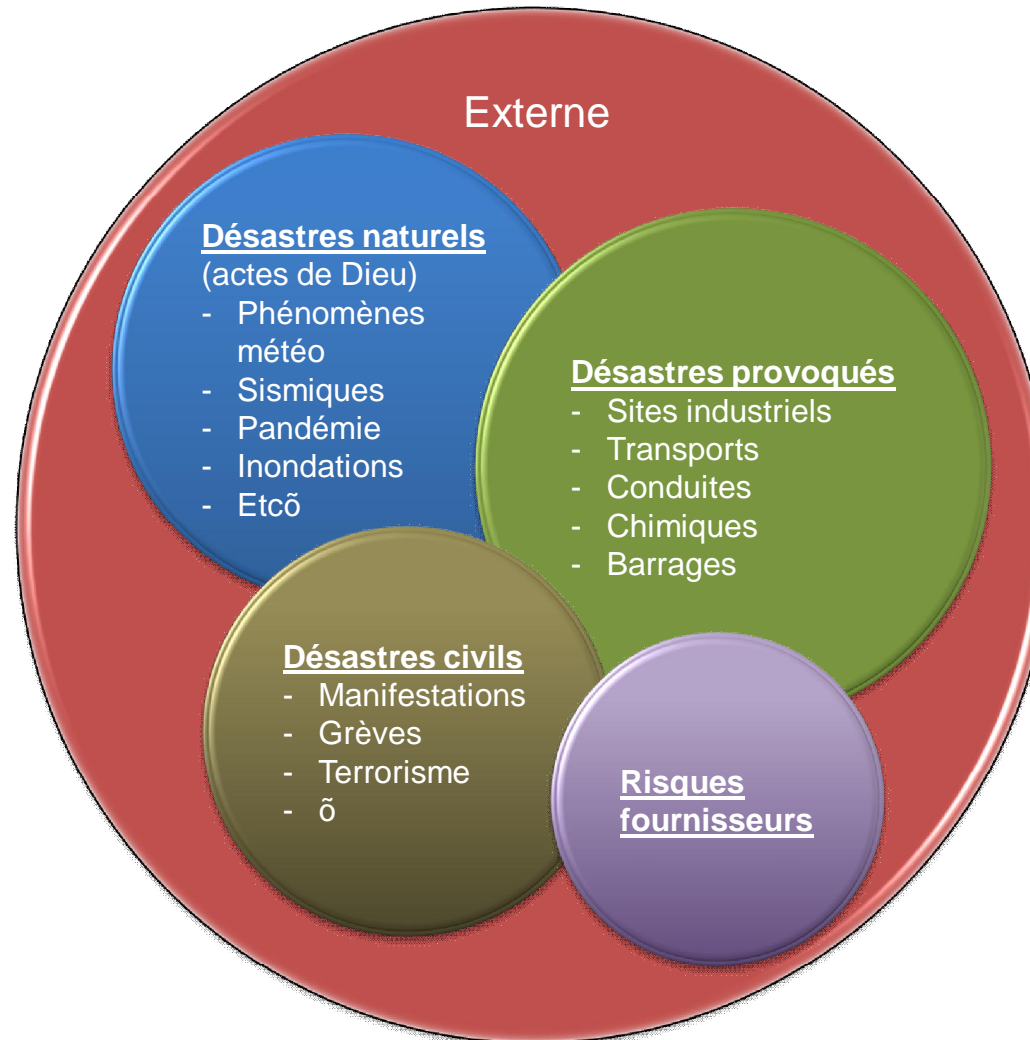
Taxonomie des sinistres et désastres

Portée



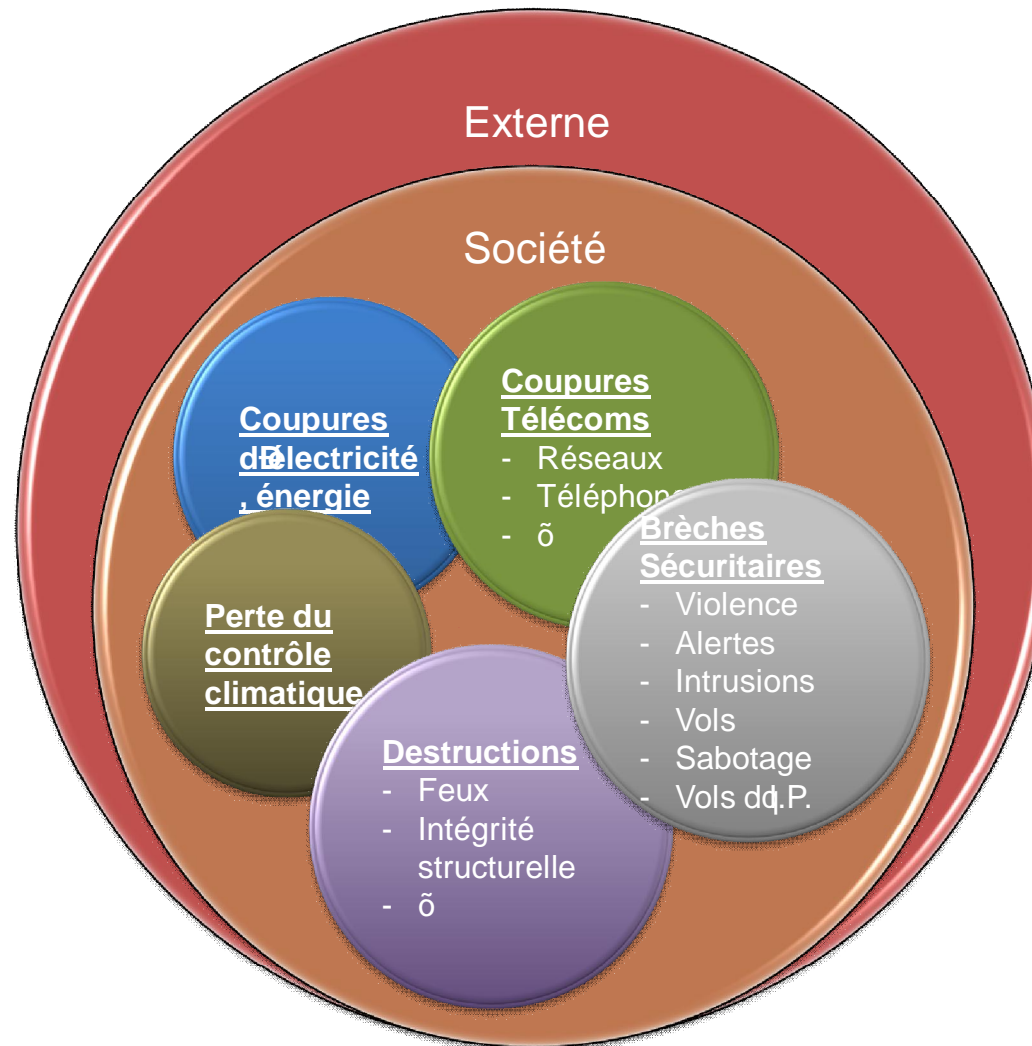
Taxonomie des sinistres et désastres

Portée - externe



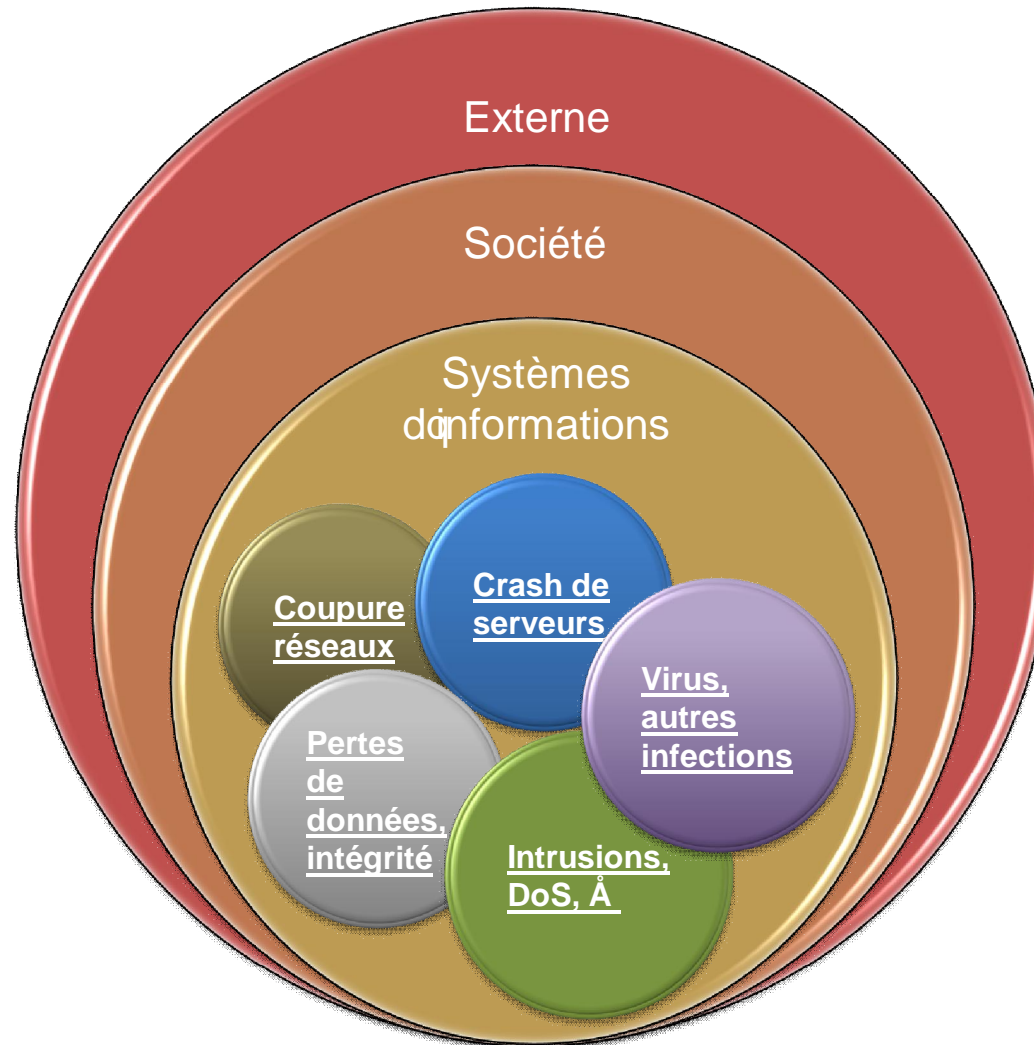
Taxonomie des sinistres et désastres

Portée - société



Taxonomie des sinistres et désastres

Portée È systèmes d'information



Dommmages 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

\$\$



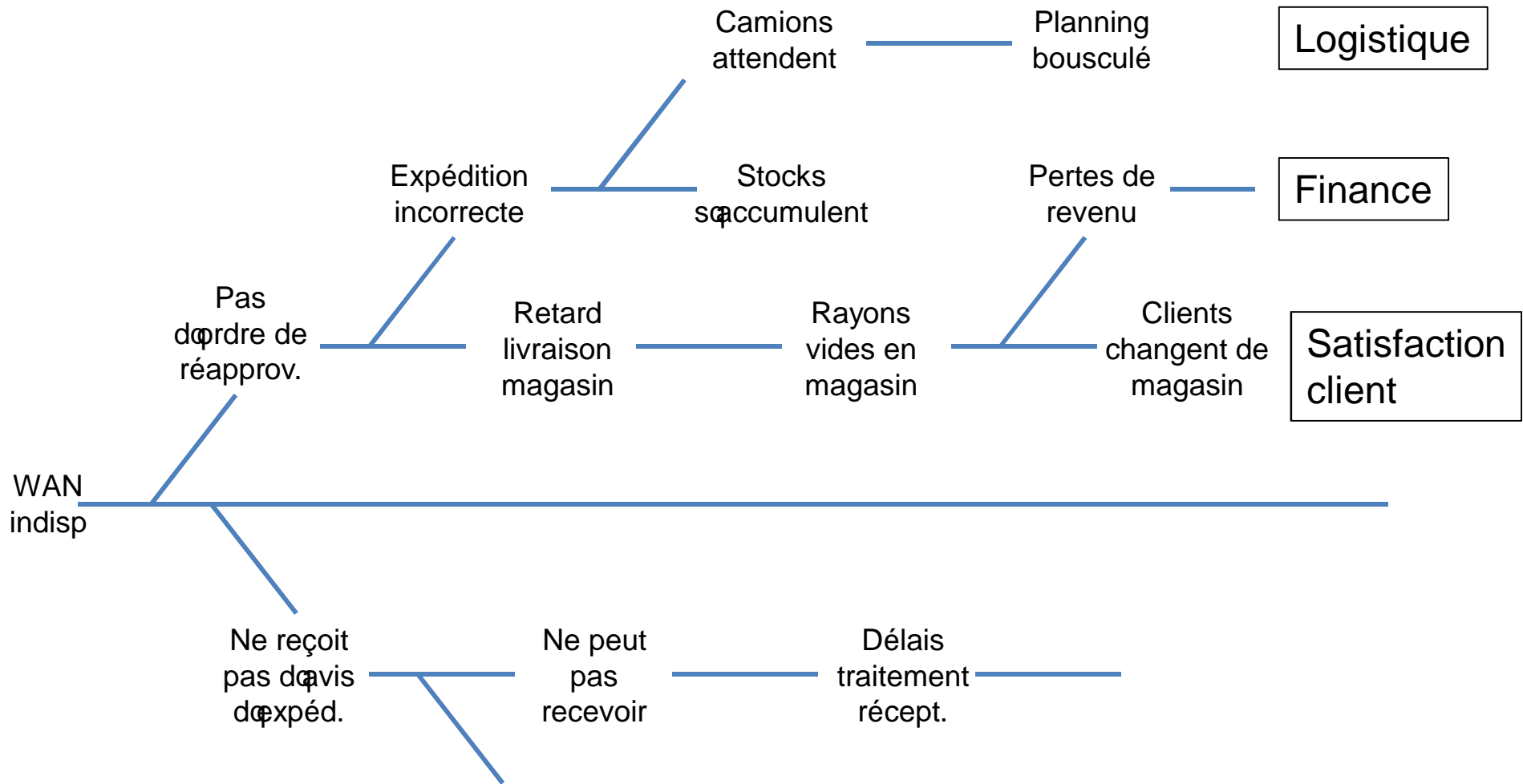
Effets à long terme

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

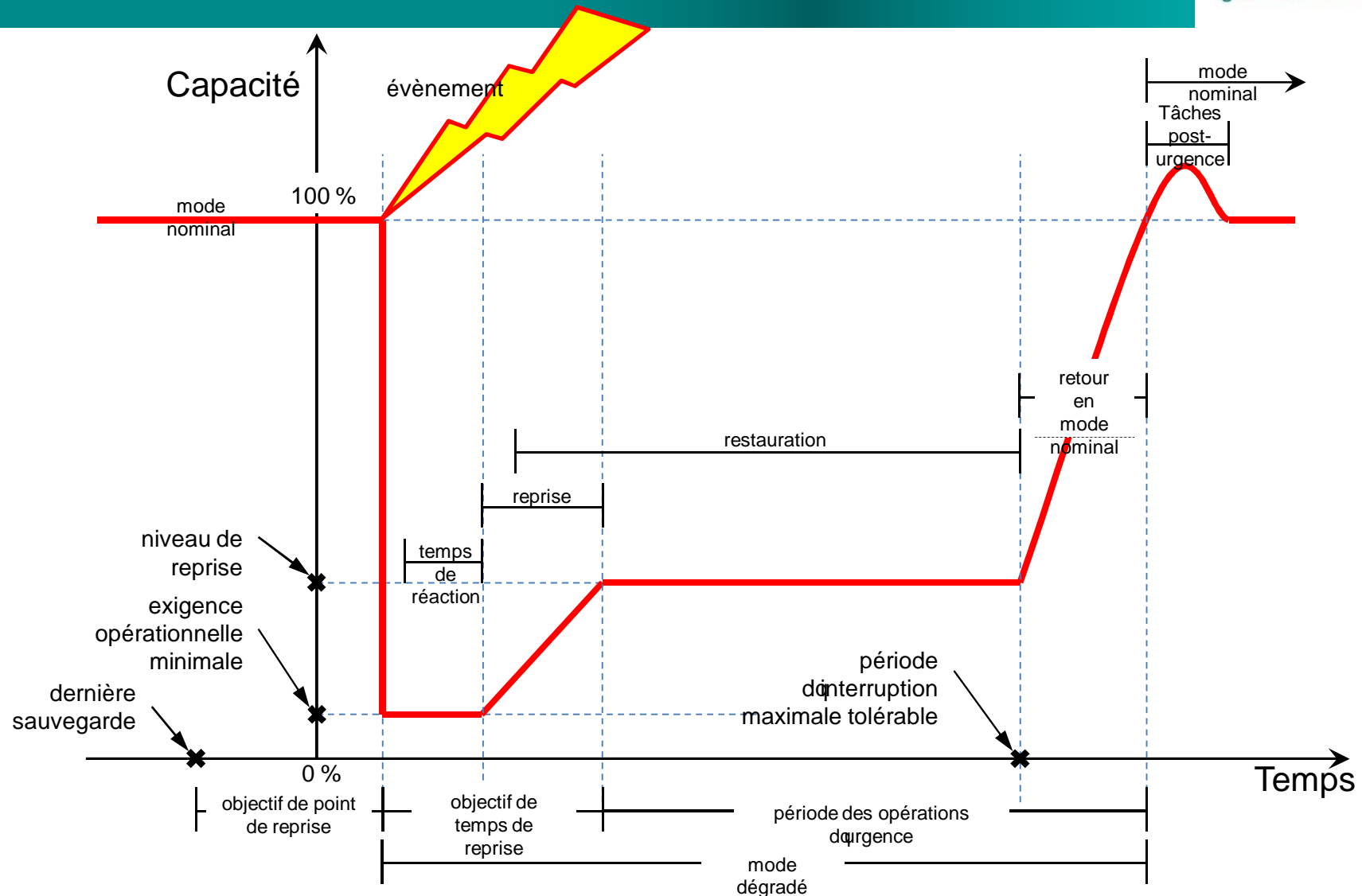
\$\$\$

Dommmages et conséquences

Diagramme d'effet (exemple)



Anatomie d'une situation de continuité





SECTION 2 – DEVELOPPER
LA RESILIENCE

Objectif de la résilience



re-sil-i-ence

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

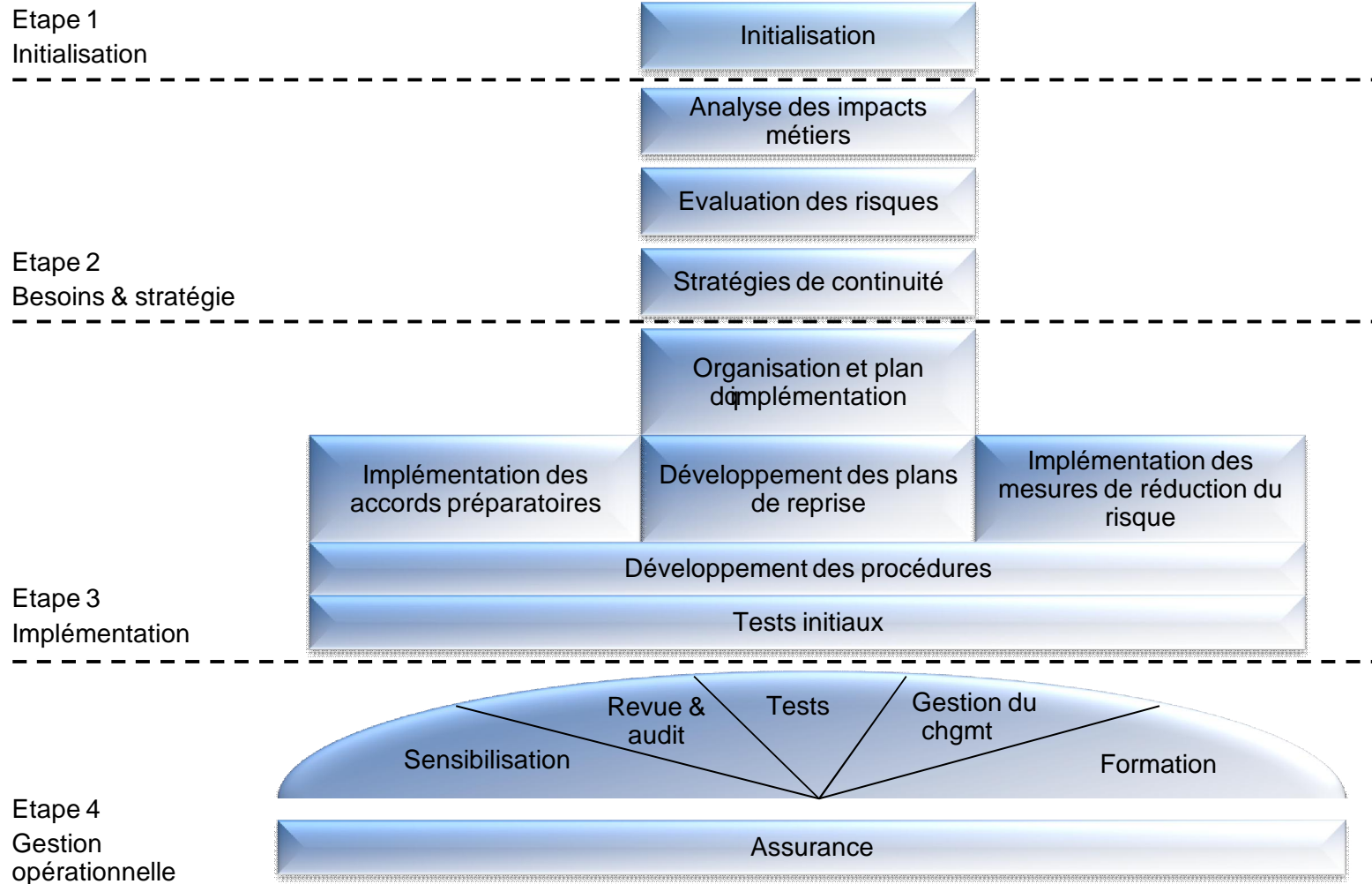


Les capacités internes de l'entreprise

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

Etape 2
Besoins & stratégies

Analyse des impacts
métiers

Evaluation des risques

Stratégies de continuité

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 ?

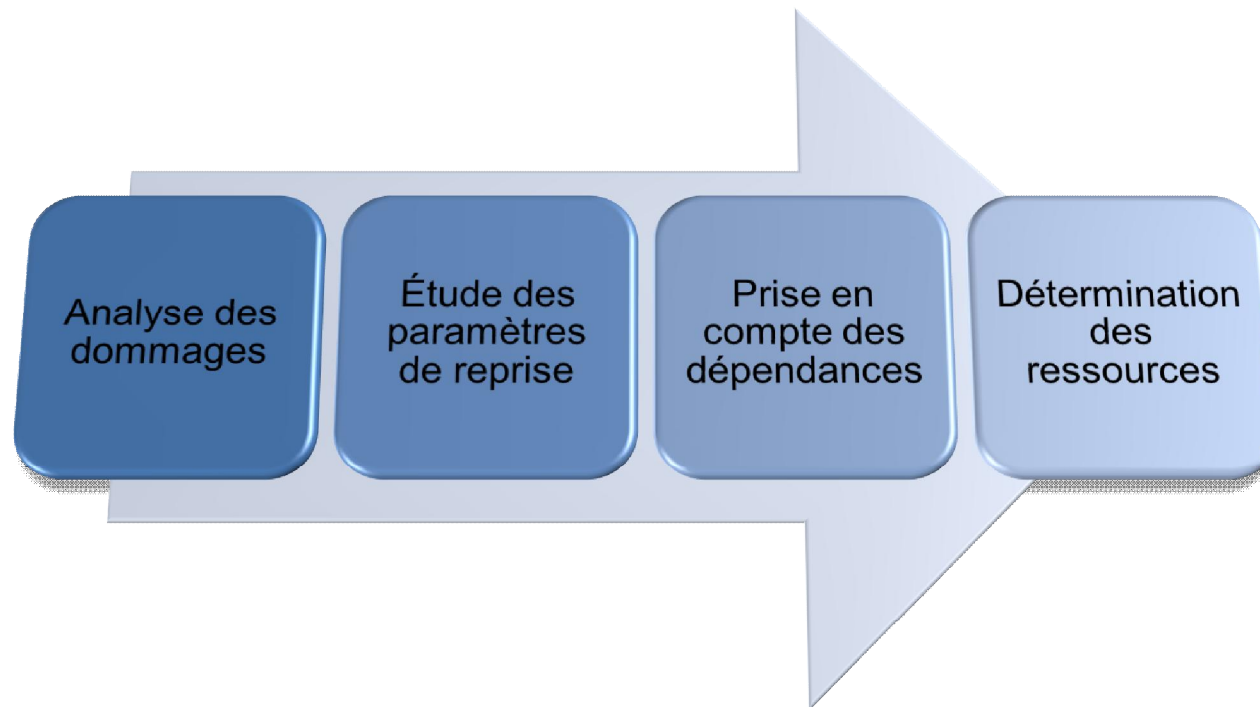
Processus général : besoins et stratégies

Etape 2
Besoins & stratégies

Analyse des impacts
métiers

Evaluation des risques

Stratégies de continuité



Rapport
d'analyse
des impacts
métiers

Processus général : besoins et stratégies

Etape 2
Besoins & stratégies

Analyse des impacts
métiers

Evaluation des risques

Stratégies de continuité

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

Identification
des risques

Évaluation
des risques

Traitement
des risques

Rapport
d'analyse
des risques

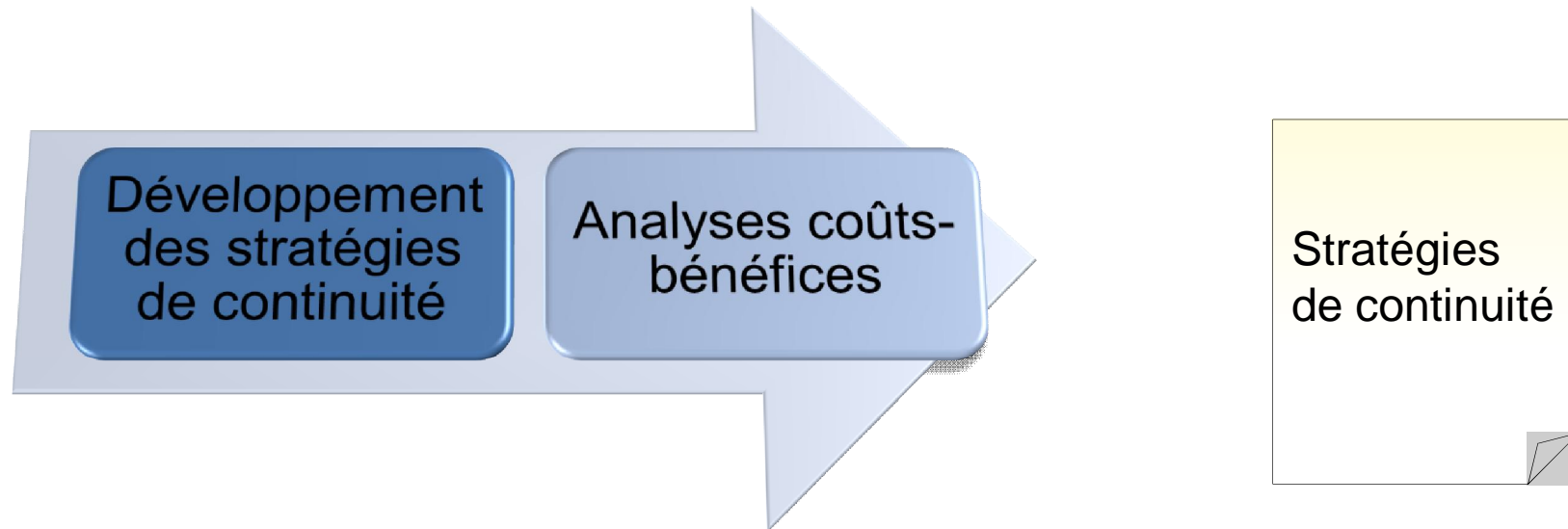
Processus général : besoins et stratégies

Etape 2
Besoins & stratégies

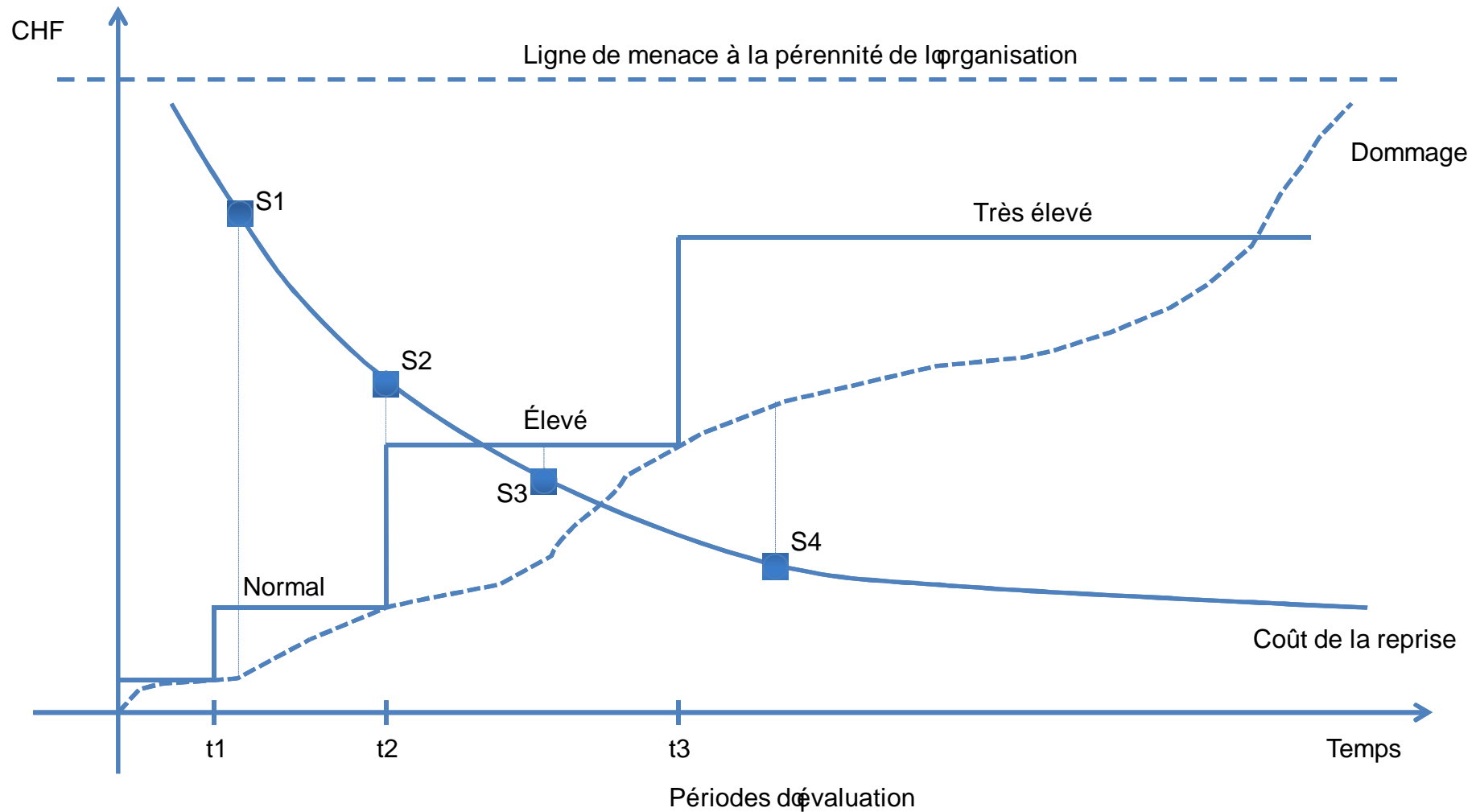
Analyse des impacts
métiers

Evaluation des risques

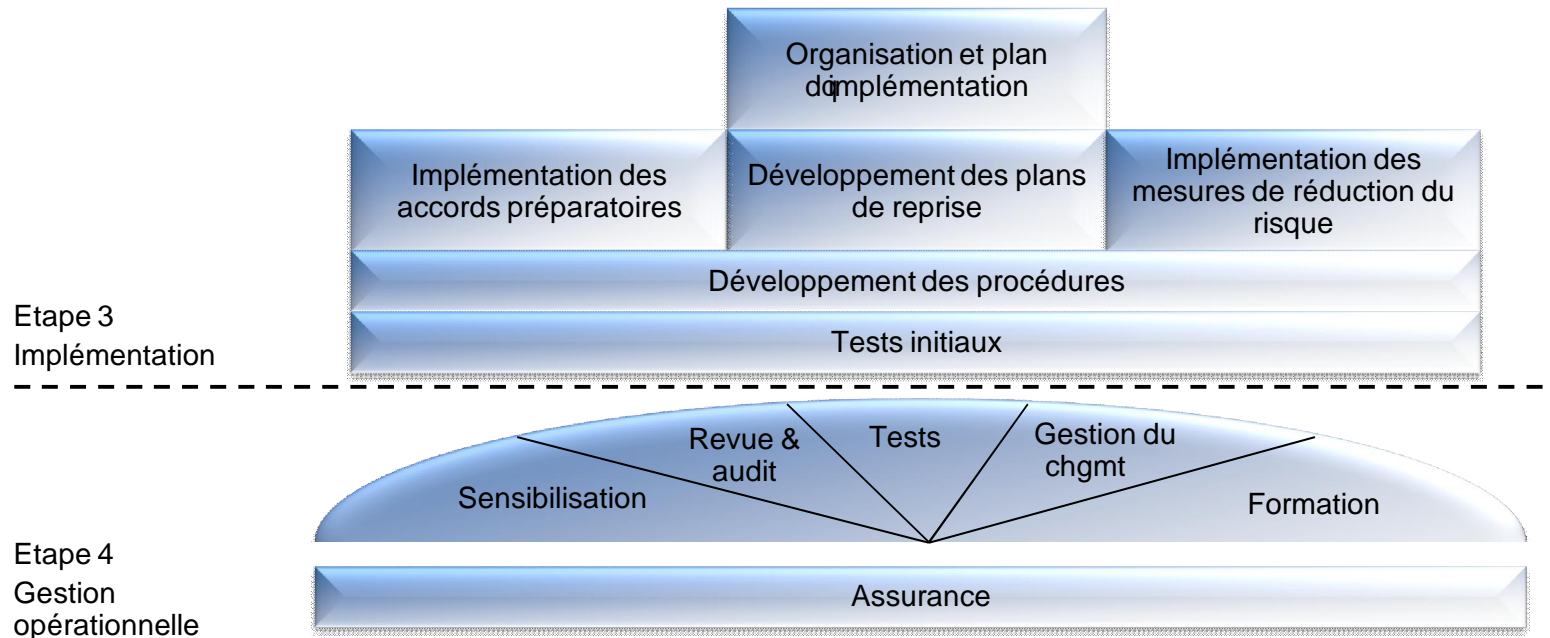
Stratégies de continuité



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**
 - ✓ *La TC 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 CONSIDÉRERAS**
 - ✓ *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 préférera 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

	<p>NFPA 1600 (2007) : Standard on Disaster/Emergency management and Business Continuity Programs NIST SP800-34 (2002) : Contingency planning guide for information technology systems</p>
	<p>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 . manging disruption-related risks</p>
	<p>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</p>
	<p>AFNOR BP Z74-700 : plan de continuité d'activité (PCA)</p>
	<p>BSI . IT Grundschutz 100-4 : Business Continuity Management</p>
	<p>ANSI/ASIS SPC.1-2009 Organizational Resilience . Security, Preparedness & Continuity Management Systems</p>
	<p>ISO/PAS 22399:2007 Guideline for incident preparedness and operational continuity management</p>

The Business Continuity Institute

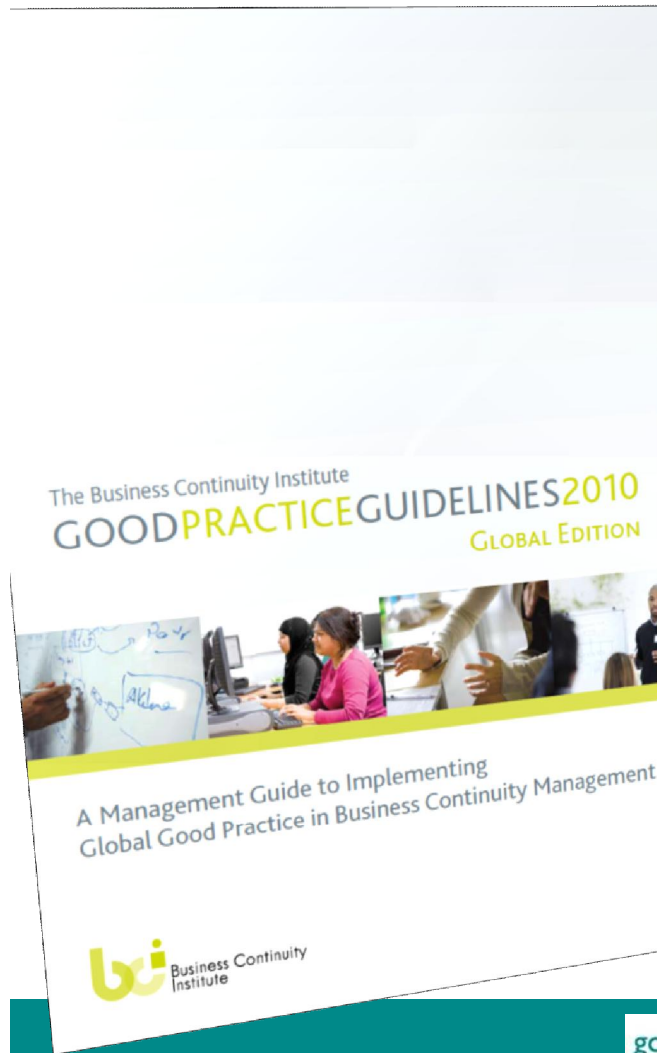


The screenshot shows the homepage of the Business Continuity Institute (BCI) website. The browser address bar displays 'http://www.thebci.org/'. The page features a blue header with the BCI logo and the text 'Business Continuity Institute Promoting the art and science of Business Continuity Management worldwide'. Below the header, there are several content blocks: a 'Members login' section with an 'Enter secure area' button; a 'Workshops' section with a 'Click for more details' button; a 'BCI CERTIFICATE' section with a 'MORE DETAILS' button; a 'BCI player' section with the text 'Film and audiovisual resources'; a 'NORDIC SYMPOSIUM 2011' section; a central navigation column with three BCI logos; a 'setting the professional standard' section with links to 'About the BCI', 'Join the BCI', 'BCI Certification', 'BCI Chapters', 'BCI Regional Forums', 'BCI News', 'BCI Mentor Scheme', 'Joint Ventures', 'Guides for BC Practitioners', 'FAQs', and 'Consultancy register'; a 'development tools for best practice in bcm' section with links to 'Good Practice Guidelines', 'BS25999 and other Standards', 'BCI E-Learning', 'BCI Training', 'BCI Accredited Training', 'BCI Benchmark', 'BCM World Conference and Exhibition', 'BCI Workshops', 'Industry Vacancies', 'Bookstore', and 'Conference Diary'; a 'corporate excellence in business continuity management' section with links to 'BCI Partnership', 'Current partners', 'Virtual exhibition', 'Industry News', 'Current Thinking', 'Continuity Magazine', 'Special Interest Groups', 'Awareness Raising', 'Resources', and 'Campaigns'; a 'bcaw business continuity awareness week 2011' section with 'Worldwide events: March 21st to 25th'; a '10-11 MAY 2011' section; a 'bum WORLD CONFERENCE AND EXHIBITION' section with '9th and 10th Nov Olympia, London, UK'; a 'Continuity' section with 'Read your copy here'; and an 'Upcoming BCI Training Courses' section. The footer contains a copyright notice '© BCI 2011' and navigation links for 'Glossary', 'Bookstore', 'News', 'Contact', 'Links', 'Privacy', and 'Site Map'.

The Business Continuity Institute : Ressources



Good Practices Guidelines 2010 :



Technical Professional Practices

Incident Response Structure

Introduction

Regardless of the cause the incident which causes a business interruption or impact, there must be a documented and fully understood incident response structure in place. This structure will cover three types or levels of management activities:

- Strategic
- Tactical
- Operational

The response structure adopted by an organization needs to address all these levels, and for each plan that is developed and implemented as part of the structure, a response team with clear procedures for escalation and control needs to be established.

An example of this is the technique used by the UK Emergency services, who define these three levels of incident response as Gold, Silver and Bronze. When applied to an organization's response structure the responsibilities of this model are shown (see below).

This model is only one example of a suitable response structure, although the need to escalate information upwards and communicate decisions downwards is an essential feature in any response model. The approach is particularly effective in the two initial phases associated with BCP implementation - Emergency Response and Incident Management.

Incident Management Plan (IMP)

Although this is part of the Business Continuity Planning process, it is often considered as a unique BCP in its own right. It has some special characteristics which differentiate it from the tactical and operational plans which form the bulk of the BCP portfolio. It is defined as:

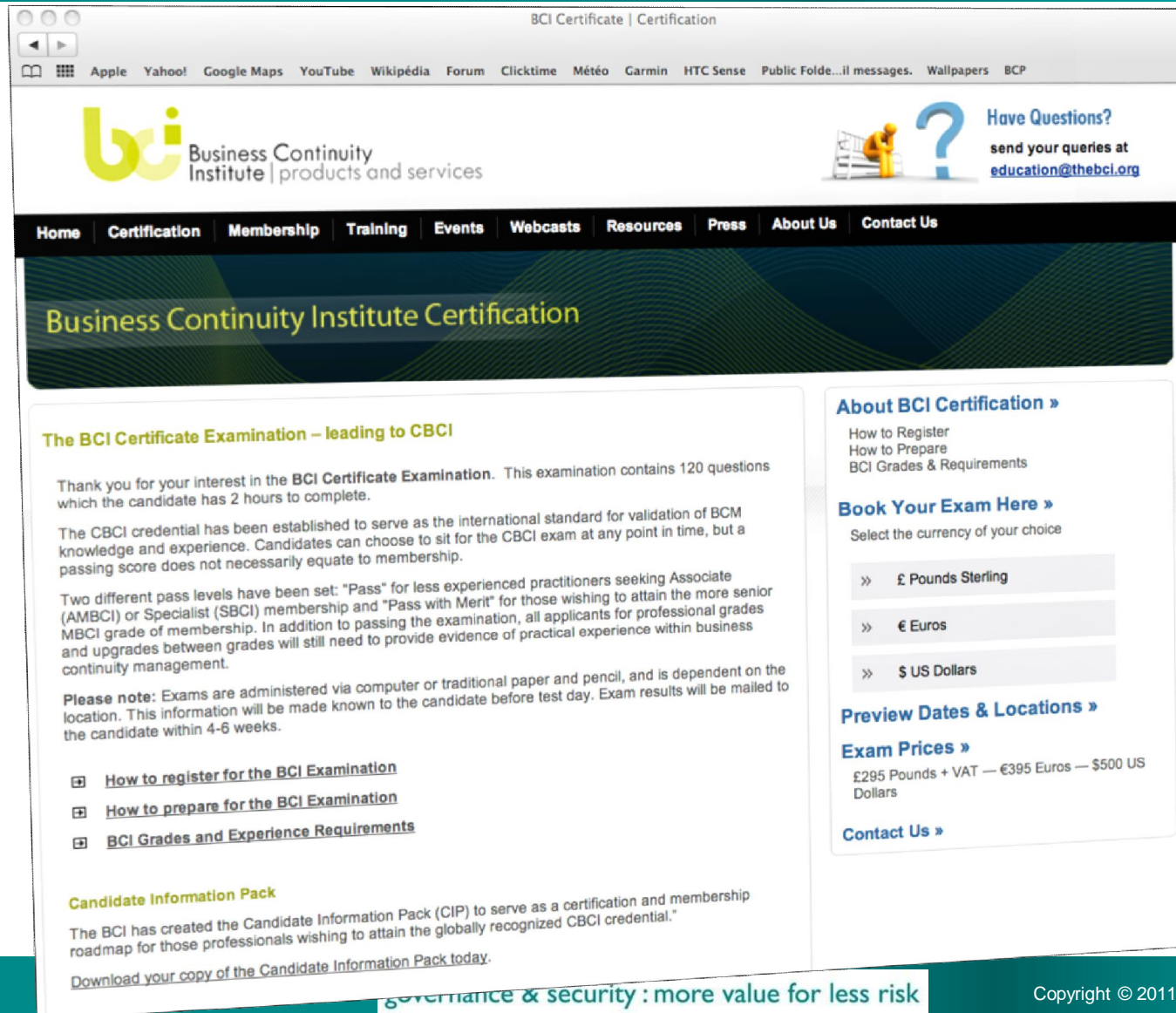
A documented plan of action for use at the time of an incident, covering key personnel, resources, services and actions needed to implement the incident management process.

This is a strategic level BCP that defines how strategic issues resulting from a major incident would be addressed and managed by Top Management. The plan may also be used when the incident is not entirely within the scope of the BCM programme. This might include crises that do not result from interruptions, such as a hostile take-over or negative media exposure, and those where the impact is over a wider area than allowed for in the BCM strategy, such as a national emergency.

The media response to any incident is usually managed at the strategic level, though some organizations could manage it at a tactical level.

The IMP is sometimes called a 'Crisis Management Plan', however reporting in the media that an organization has invoked its 'Crisis Management Team' may lead people to think the organization feels that it has a 'Crisis', the term 'incident' has less negative connotations so is preferred in this document.

The Business Continuity Institute : Schème de certification



The screenshot shows a web browser window with the URL "BCI Certificate | Certification". The browser's address bar and search bar are visible at the top. The page features the BCI logo and the text "Business Continuity Institute | products and services". A navigation menu includes links for Home, Certification, Membership, Training, Events, Webcasts, Resources, Press, About Us, and Contact Us. The main content area is titled "Business Continuity Institute Certification" and contains the following text:

The BCI Certificate Examination – leading to CBCI

Thank you for your interest in the **BCI Certificate Examination**. This examination contains 120 questions which the candidate has 2 hours to complete.

The CBCI credential has been established to serve as the international standard for validation of BCM knowledge and experience. Candidates can choose to sit for the CBCI exam at any point in time, but a passing score does not necessarily equate to membership.

Two different pass levels have been set: "Pass" for less experienced practitioners seeking Associate (AMBCI) or Specialist (SBCI) membership and "Pass with Merit" for those wishing to attain the more senior MBCI grade of membership. In addition to passing the examination, all applicants for professional grades and upgrades between grades will still need to provide evidence of practical experience within business continuity management.

Please note: Exams are administered via computer or traditional paper and pencil, and is dependent on the location. This information will be made known to the candidate before test day. Exam results will be mailed to the candidate within 4-6 weeks.

- How to register for the BCI Examination
- How to prepare for the BCI Examination
- BCI Grades and Experience Requirements

Candidate Information Pack

The BCI has created the Candidate Information Pack (CIP) to serve as a certification and membership roadmap for those professionals wishing to attain the globally recognized CBCI credential.

[Download your copy of the Candidate Information Pack today.](#)

About BCI Certification »

- How to Register
- How to Prepare
- BCI Grades & Requirements

Book Your Exam Here »

Select the currency of your choice

- » £ Pounds Sterling
- » € Euros
- » \$ US Dollars

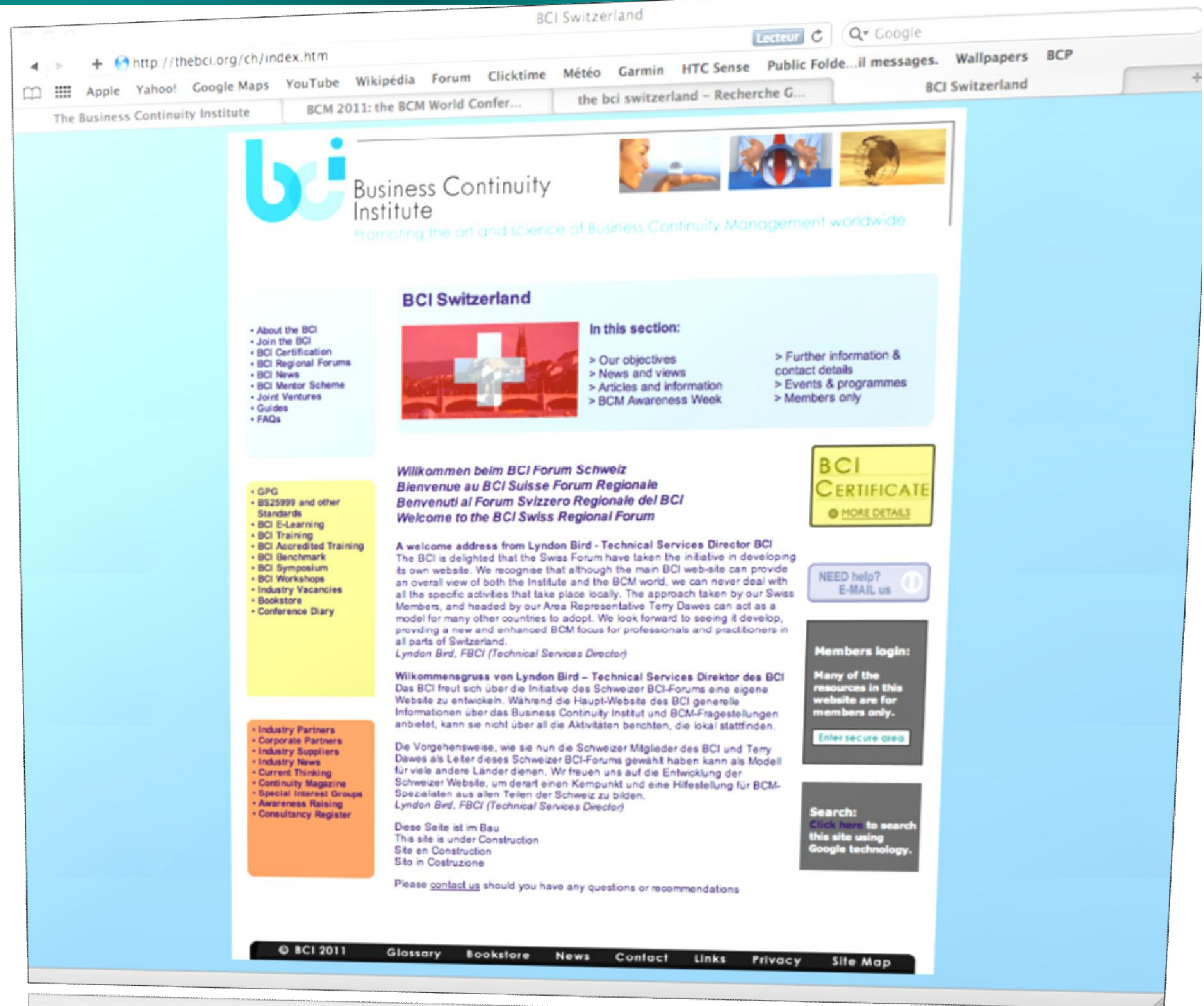
Preview Dates & Locations »

Exam Prices »

£295 Pounds + VAT — €395 Euros — \$500 US Dollars

Contact Us »

The Business Continuity Institute : Publications et chapitres locaux



more value for less risk !



Merci pour votre attention !

***Nous restons à votre disposition pour toute
questions ou informations***

Pour nous contacter :
info@ardantic.ch

Services d'ardantic



more value for less risk !



Merci pour votre attention !

***Nous restons à votre disposition pour toute
questions ou informations***

Pour nous contacter :
info@ardantic.ch