

Réponse à incident

Introduction du module

Présentation générale

Objectifs



1. Comprendre les enjeux d'une crise cybersécurité dans l'organisation
2. Déterminer les activités critiques de l'organisation, les risques encourus et les plans d'actions permettant la continuité d'activité
3. Participer à la gestion de crise
4. Documenter la gestion de crise
5. Réaliser un retour d'expérience sur la crise et ses procédures de gestion

Présentation générale

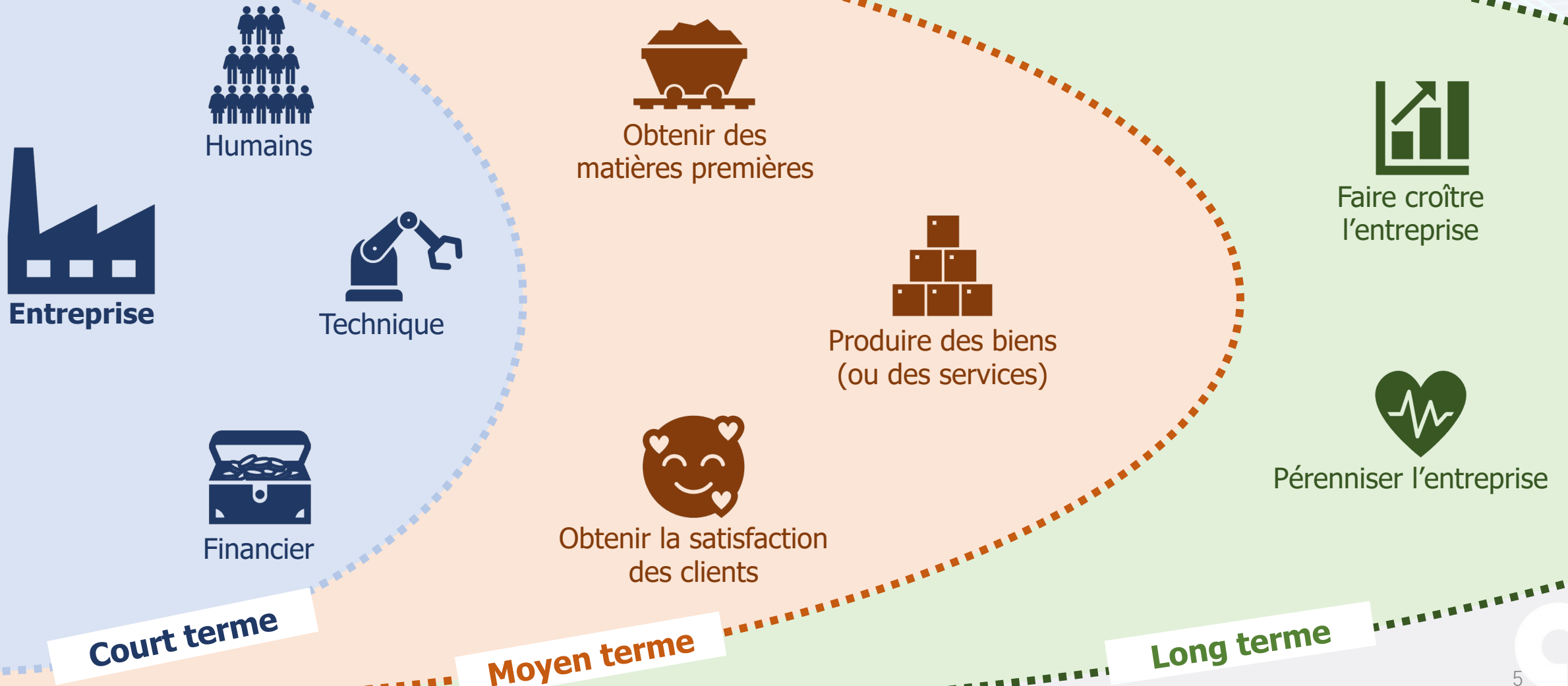
Présentation des séquences

- 1** Comprendre la gestion de crise cyber
- 2** Organiser et gérer une crise cyber
- 3** Mettre en place un plan de continuité et de reprise d'activité
- 4** Gérer la communication de crise

Les risques opérationnels et la perturbation de l'activité

Les fondements de la continuité d'activité

Risques opérationnels



Les fondements de la continuité d'activité

Les entreprises sont préoccupées par la maîtrise de leurs risques opérationnels

Risques de pertes



Processus internes inadéquats ou défectueux



Personnes et systèmes ou événements externes

Ils peuvent affecter ou nuire gravement le fonctionnement ou la pérennité de l'entreprise

La notion de risques opérationnels

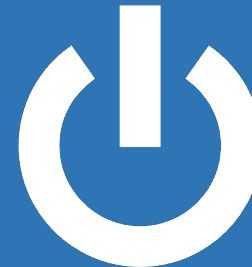
**Sinistre
majeur**

Événement portant sur les biens et/ou les personnes et pouvant mettre en péril la pérennité de l'entreprise

Les défis principaux pour une entreprise en cas de sinistre majeur



Assurer la continuité des opérations



Relancer les opérations au plus vite en cas d'interruption

Notions fondamentales de la continuité d'activité

The background features a dark blue gradient with intricate, glowing teal wavy lines that resemble topographical contours or sound waves. In the lower-left corner, there is a large, semi-transparent teal sphere with a smaller, solid teal sphere positioned just below it. The overall aesthetic is modern and scientific.

La définition d'un plan de continuité d'activité

Ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris **face à des chaos extrêmes**, le **maintien**, le cas échéant de façon temporaire selon un **mode dégradé**, des prestations de services **essentiels** de l'entreprise, puis la **reprise planifiée** des activités

CRBF 2004/02



La définition d'un plan de continuité d'activité

Procédures documentées servant de guide aux organisations pour **répondre, rétablir, reprendre et retrouver un niveau de fonctionnement** prédéfini à la suite d'une perturbation

ISO 22301



Les objectifs et les scénarios de la continuité d'activité

Ensemble des processus visant à assurer le fonctionnement de l'entreprise en cas de sinistre majeur



Objectifs

- Résister aux événements externes à l'activité pouvant interrompre durablement les opérations ou causer des dommages importants
- Mettre en œuvre des solutions pour redémarrer en mode dégradé dans des délais tolérable
- Apporter le dimensionnement nécessaire à la continuité d'activité



Scénarios couverts

- Perte des locaux utilisateurs et/ou informatique
- Perte du système d'information
- Perte d'alimentation des services essentiels
- Défaut d'un fournisseur essentiel
- Crise sanitaire

Le PCA couvre à la fois des problématiques métiers et IT

Ces scénarios relèvent-ils du PCA ?

Incendie du site informatique principal d'une entreprise d'assurance

Ces scénarios relèvent-ils du PCA ?

Arrêt d'un puit de pétrole pour une société d'exploitation pétrolière

Ces scénarios relèvent-ils du PCA ?

**Chute du cours d'une devise pour une banque
d'investissement**

Ces scénarios relèvent-ils du PCA ?

Inaccessibilité des locaux utilisateurs

Ces scénarios relèvent-ils du PCA ?

Coupure électrique de longue durée

Ces scénarios relèvent-ils du PCA ?

Bug dans un logiciel pour une société de développement logiciel

Les enjeux de la mise en œuvre d'un PCA

Trois enjeux pour une entreprise pour mettre en place un PCA



Survie de l'entreprise



Maîtrise de sa communication



Argument commercial

Les contraintes réglementaires

