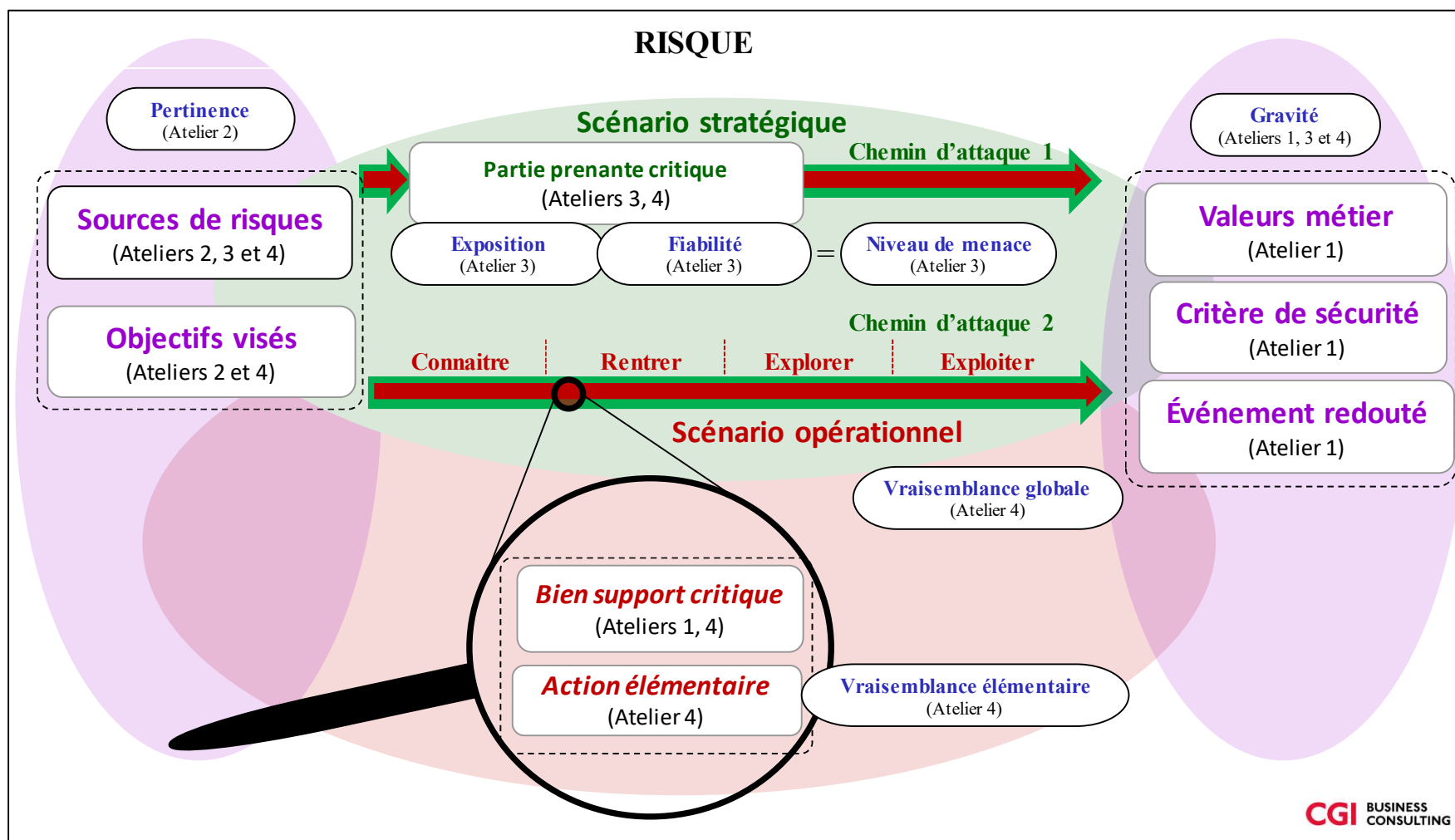
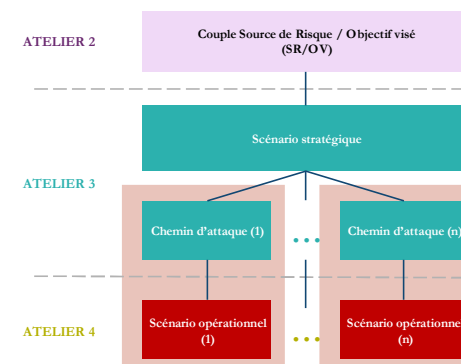


**RISQUE** : Un scénario stratégique avec un niveau donné,  
exploité par une source de risques visant un objectif (SROV),  
composé d'un ou plusieurs chemins d'attaque, utilisant ou non des  
parties prenantes comme vecteur d'attaque.  
Chaque chemin d'attaque est composé d'actions élémentaires  
constituant un scénario opérationnel



**RISQUE : Un scénario stratégique avec un niveau donné,**  
exploité par **une source de risques visant un objectif (SROV) et engendrant un évènement,**  
composé **d'un ou plusieurs chemins d'attaque, utilisant ou non des parties prenantes comme vecteur d'attaque.**  
**Chaque chemin d'attaque est composé d'actions élémentaires constituant un scénario opérationnel**

#### Gravité

Estimation du niveau et de l'intensité des effets d'un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects.

#### Vraisemblance

Estimation de la faisabilité ou de la probabilité qu'un risque se réalise, selon l'échelle adoptée (très faible, peu vraisemblable, quasi certain, etc.).

#### Valeur métier

Dans le cadre de l'étude, composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé.

#### Evènement redouté

Un évènement redouté est associé à une valeur métier et porte atteinte à un critère ou besoin de sécurité de la valeur métier (exemples : indisponibilité d'un service, modification illégitime du seuil de température haute d'un processus industriel, divulgation de données classifiées, modification d'une base de données). Les événements redoutés à exploiter sont ceux des scénarios stratégiques et se rapportent à l'impact d'une attaque sur une valeur métier. Chaque événement redouté est évalué selon le niveau de gravité des conséquences, à partir d'une métrique.

#### Source des risque

Élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque. Une source de risque peut être caractérisée par sa motivation, ses ressources, ses compétences, ses modes opératoires (de prédilection). Exemples : services étatiques, hacktivistes, concurrents, employés vengeurs.

#### Objectif visé

Finalité visée par une source de risque, selon ses motivations.  
Exemples : voler des informations à des fins lucratives ou d'espionnage industriel, diffuser un message idéologique, se venger d'un organisme, générer une crise sanitaire.

#### Scénario stratégique

Chemins d'attaque allant d'une source de risque à un objectif visé en passant par l'écosystème et les valeurs métier de l'objet étudié. Les scénarios stratégiques sont évalués en termes de gravité.

#### Partie prenante

Élément de l'écosystème (personne, système d'information ou organisation) qui est externe à l'objet de l'étude (dont la MOA n'est pas partie prenante dans les décisions de traitement des risque). Elle devient **critique** lorsqu'elle est susceptible de constituer un vecteur d'attaque privilégié.

#### Chemin d'attaque

Suite d'événements distincts que la source de risque devra probablement générer pour atteindre son objectif. Cette terminologie concerne les scénarios stratégiques.

#### Scénario opérationnel

Enchaînement d'actions élémentaires portées sur les biens supports de l'objet étudié ou de son écosystème. Planifiés par la source de risque en vue d'atteindre un objectif déterminé, les scénarios opérationnels sont évalués en termes de vraisemblance

#### Action élémentaire

Action unitaire exécutée par une source de risque sur un bien support dans le cadre d'un scénario opérationnel.  
Exemples : exploiter une vulnérabilité, envoyer un email piégé, effacer des traces, augmenter des privilèges.

#### Bien support

Composante du système d'information sur laquelle repose une ou plusieurs valeurs métier. Un bien support peut être de nature numérique, physique ou organisationnelle.

Exemples : serveur, réseau de téléphonie, passerelle d'interconnexion, local technique, dispositif de vidéo protection, équipe en charge du projet, Administrateurs, département R&D. Il devient **critique** quand il est jugé très susceptible d'être ciblé par une source de risque pour atteindre son objectif. Les biens supports critiques sont ceux qui apparaissent dans les scénarios opérationnels