

La gestion des risques des tierces-parties

5 à 7 du Clusis




CLUSIS

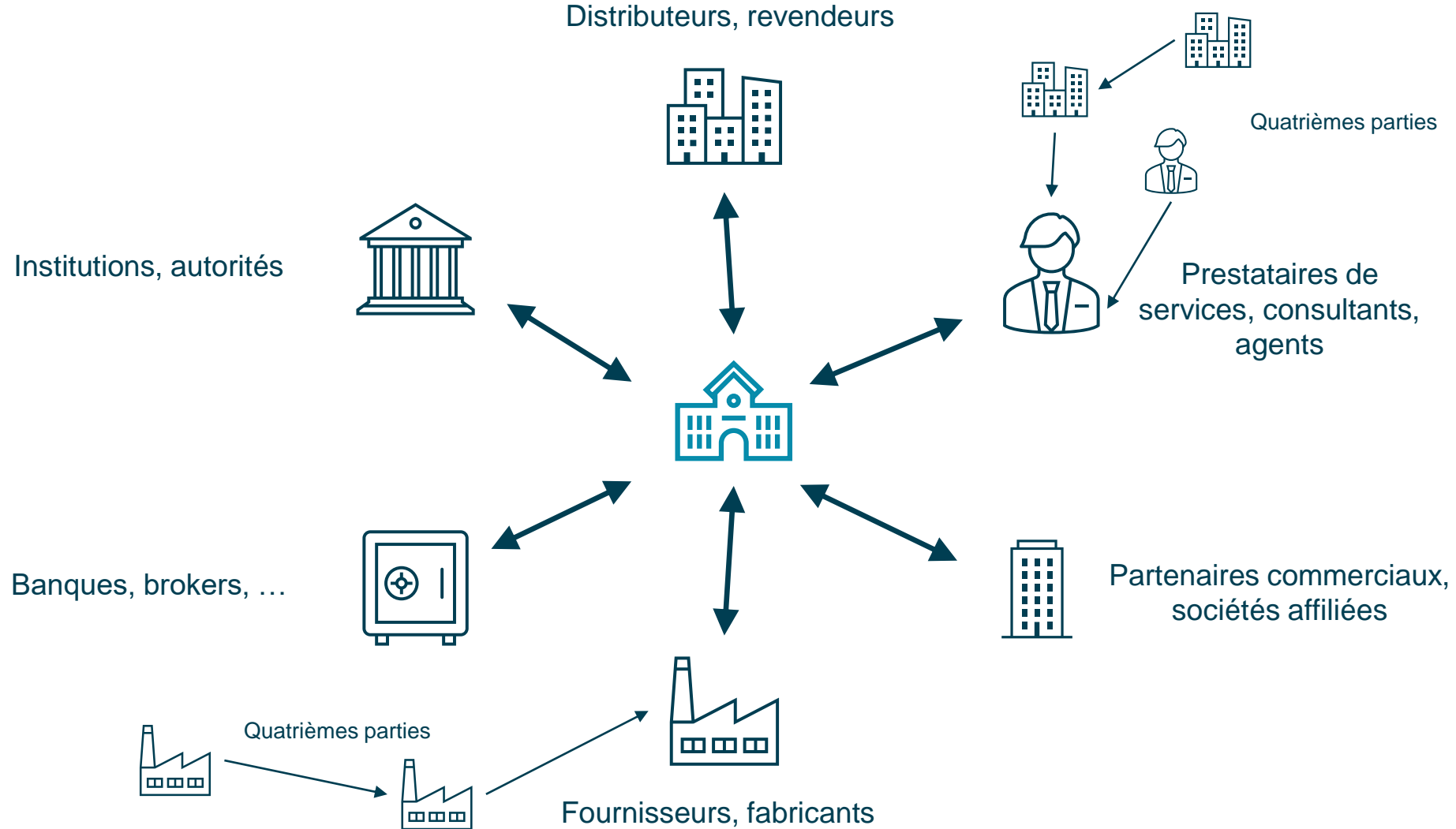
24 Janvier 2023

Sommaire



- La gestion des risques des tierces-parties (VRM ou TPRM)
- Pourquoi gérer les risques des tierces-parties
- Les bonnes pratiques en gestion des risques des tierces-parties
- La classification ou le Vendor Tiering
- Questionnaires et checklists
- Des services managés
-  SUPPLIER SHIELD

Les tierces-parties



Les risques des tierces-parties

Avantages stratégiques, économies, expertise



Risques financiers, réputationnels, opérationnels

Les risques des tierces-parties

1. La tierce partie comme tremplin
2. Extension latérale
3. Insuffisance du périmètre de surveillance
4. Risque tout au long du cycle de vie de la donnée



Non-conformités légales
ou réglementaires



Fuite de données
personnelles



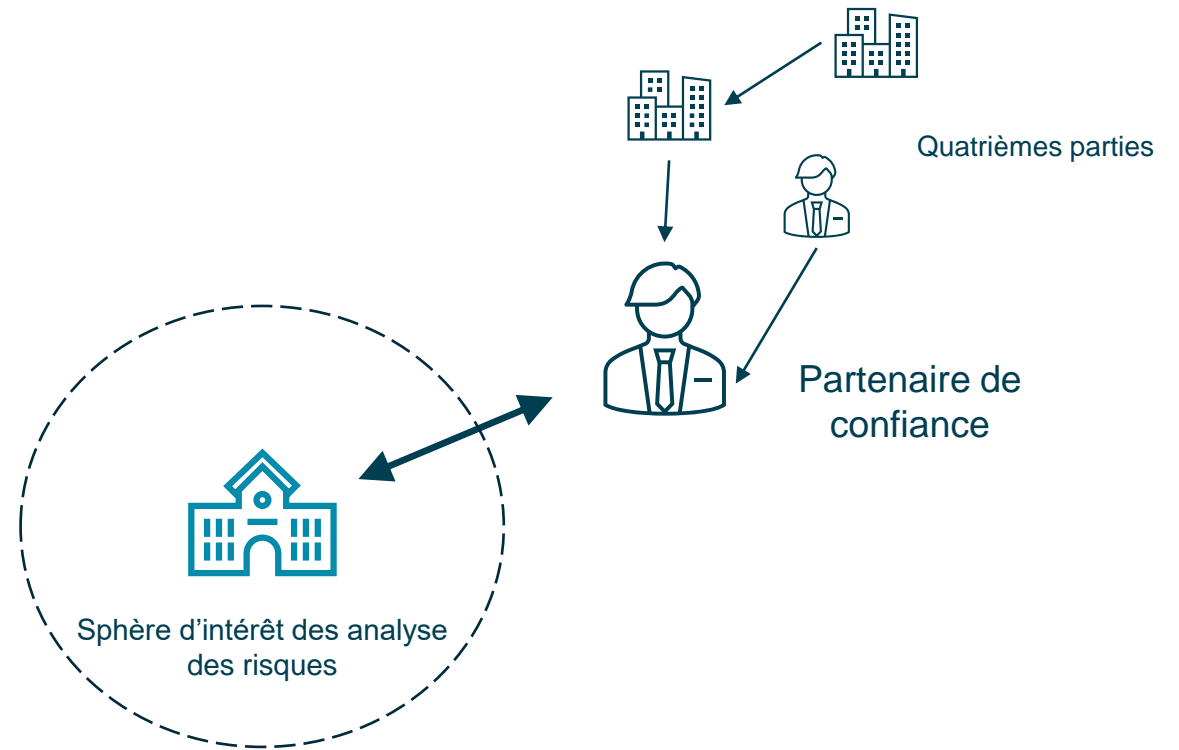
Brèche de sécurité de
l'information



Perte ou vol de propriété
intellectuelle



Rupture de contrat,
procès



L'évolution de l'écosystème des tierces-parties

1. Extension de la sous-traitance sur des fonctions stratégiques (ventes, marketing, distribution, SAV)
2. Multiplication des plateformes de collaboration & taux de pénétration et de dépendance accrus
3. Évolution de la nature des tâches accomplies vers le plus critique



4. Tendance marquée à poursuivre l'externalisation vers le low-cost & far-shore
5. Compartimentalisation des services mais consolidation des sous-traitants

Pourquoi gérer les risques des tierces-parties

RESPONSABILITÉS

La repartition des responsabilités entre la société et les tierces-parties est Claire, comprise et appliquée

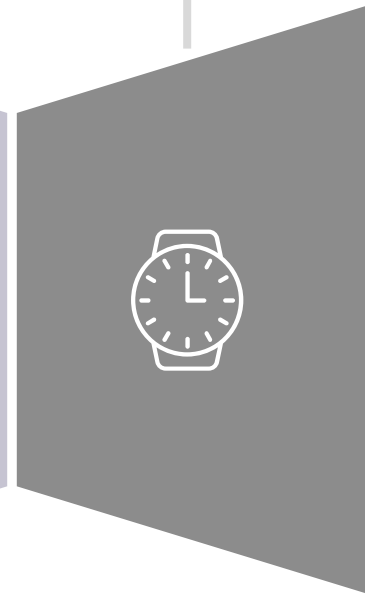
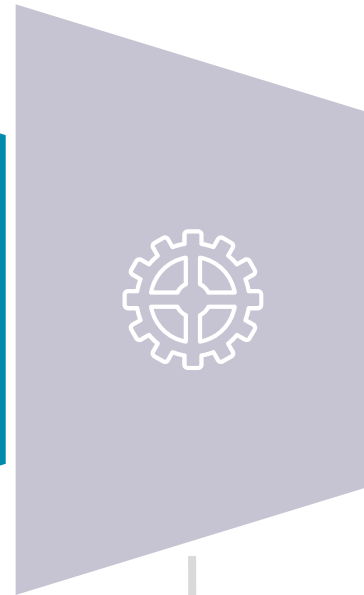


MAÎTRISE DES RISQUES

Gérer les risques présents et futurs prend moins de temps et de ressources
Les risques sont effectivement réduits

COÛTS OPTIMISÉS

La prevention vaut bien mieux que la reparation
Les coûts d'incidents sont réduits

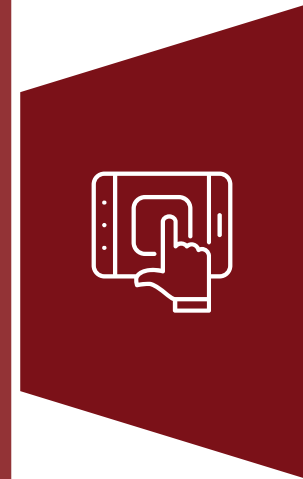


QUALITÉ & DISPONIBILITÉ

On réduit les risques de perte de qualité ou de disponibilité du service

CONFORMITÉ

Réglementations et standards imposent une gestion des risques des tierces-parties (SOX, HIPOAA, PCI DSS, NIS 2, ...)



EFFICIENCE

On s'assure une efficacité opérationnelle et financière

Bonnes pratiques en gestion des risques des tierces-parties

Inventaire
systématique des
tierces-parties

**Registre des
risques** posés par
les tierces-parties

Segmentation
des tierces-parties
par niveaux de
risques

Déploiement de
« plateaux » par
importance et
niveaux de
risques

Évaluations
systématiques des
nouvelles tierces-
parties à l'aune des
exigences de
sécurité

Responsabilisation
par la désignation du
porteur de risques en
interne

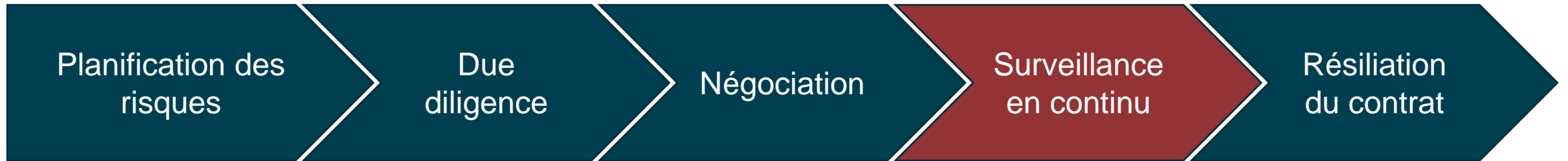
**Formation et
sensibilisation** de
tous les acteurs
interagissant avec
les tierces-parties

Audit interne
annuel de chaque
tierce-partie
considérée comme
critique par une
entité indépendante

Plan de réponse à
exécuter lorsqu'une
brèche de contrat
ou de données
survient

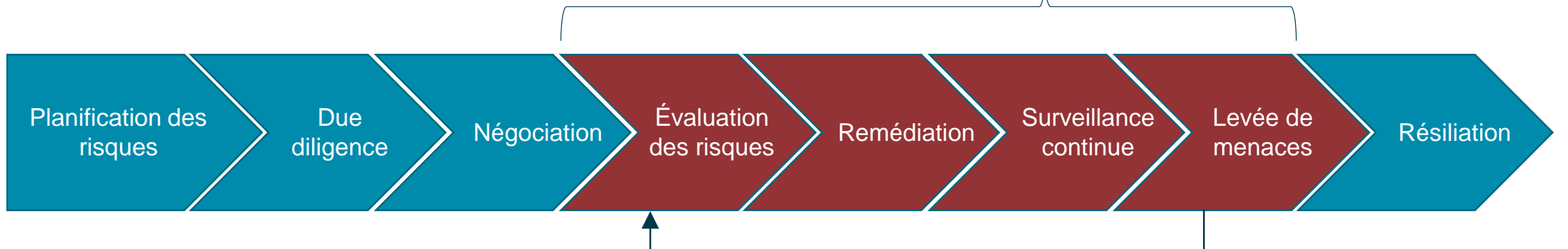
Des processus
évolutifs (**services
managés**) pour la
scalabilité du
programme de
gestion des tierces-
parties

Un nouveau cycle de vie de la gestion des tierces-parties



Amélioration continue de la posture de sécurité de la tierce-partie

Effort relatif du cycle de vie consenti à la surveillance de la performance et de la sécurité



Classification des tierces-parties – vendor tiering



Dépendance
Niveau de pénétration



Des questionnaires



Questionnaire de sécurité

Domaines



Mesures et politiques de sécurité et de protection des données



Sécurité physique, datacenters



Web apps



Infrastructure & endpoints



Contrôle des accès



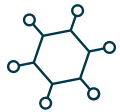
Continuité & résilience



Gestion des incidents



Gestion des risques



Menaces & vulnérabilités



Supply chain management



Lois, règlements & conformité

Sources

- ISO 27001:2022
- CIS
- NIST SP 800
- VSAQ
- Standardized Information Gathering (Shared Assessments)
- GDPR / nLPD

- PCI DSS
- HIPAA /SOX

- Custom



Peu de questions mais les bonnes questions

Bonnes pratiques



Question claire = réponse claire



Conserver les questionnaires



Favoriser les certifications



Prendre en compte les plans de remédiations

Évaluation de la sécurité de la tierce-partie

La tierce-partie

A investi dans des mesures de sécurité

Utilise un contrôle des accès

Satisfait aux exigences minimales de sécurité

A fourni les informations sur son infrastructure

Effectue régulièrement des pen-tests

Dispose de mesures de sécurité physique

N'a pas d'historique de brèches de sécurité

A un programme de formation et sensibilisation

1st

Score !!

Score de
sécurité

Benchmarking

Continuous Attack Surface
Monitoring

Niveau de risque considéré acceptable

Une gestion scalable et évolutive du TPRM



Partager les responsabilités avec les fournisseurs, c'est un travail symbiotique



Benchmarker les fournisseurs entre eux



Remplacer Excel par une plateforme de gestion des risques tiers



Assurer une bande passante suffisante pour adresser tous les tiers parties



Eviter la myopie de la surface d'attaque en évaluant les postures sécuritaires des tiers en continu

Service Managé

Compétences

Expérience

Efficience

Automatisation

SUPPLIER SHIELD

Supplier SHIELD

Overview

Suppliers

Assessments

My Account

Controls

Users

Questionnaires

Log out

Support

Hello John McClane!
Supplier chain manager

Tier 2 10/500 + Supplier Assessments available 12 + Assessment Demo request@suppliershield.com

Suppliers repository

10 / 500
Total suppliers

1 Suppliers not rated
8 Assessments available

List of Suppliers

- My company
- Baptista Group
- Best Hosting Services
- Untel
- DevSoft Ltd.

Business unit **Operations (7)**

- Business unit **Finance (2)**
- Business unit **Human resources (3)**
- Business unit **Facilities (1)**
- Business unit **Support (3)**

Sub unit **FM Champion (0)**

ACME Software

Assessments

13 Assessments

Completed	7
In evaluation	0
At supplier's	4
Draft	2
Late assessments	4

Controls

174


- Not compliant
- Partially compliant
- Compliant

Low

Critical



SUPPLIER SHIELD



SUPPLIER SHIELD

- Overview
- Suppliers**
- Assessments
- My Account
- Controls
- Users
- Questionnaires
- Log out

Tier 2 10/500 + Supplier Assessments available 12 + Assessment Demo request@suppliershield.com

All suppliers

10/500

Suppliers
1 not rated

+ New

Status

3

assessments
in progress

3

without active
assessments

3

with delayed
assessments

4

without
assessments

Risk level

High risk 2

Moderate risk 2

Tolerable 5


Not rated 1

Name	Assessments	Business unit	Exposure	Actual rating	Risk level
My company	0	EUC	High	No rating	High risk
Baptisa Group	0	EUC, Hire to retire	Low	No rating	Tolerable
Best Hosting Services	2	Sales Support	High	3 shields	Moderate risk
Untel	0	Infrastructure, Acquisitions, Payroll	Low	No rating	Tolerable
DevSoft Ltd.	2	Payroll	High	2 shields	Tolerable
Abilene Advisors S.A.	2	Security, Procurement	Medium	3 shields	Tolerable
ACME Software	3	Infrastructure, Facilities, Sales Support	Low	3 shields	Tolerable
ConnectNow!	1	Infrastructure	High	2 shields	High risk
Dodgy Ltd	3		High	No rating	Not rated
Seb Media Inc.	0	Infrastructure, Sales Support	High	No rating	Moderate risk

© Copyright 2022 Abilene Advisors

Support





SUPPLIER SHIELD

- [Overview](#)
- [Suppliers](#)
- [Assessments](#)
- [My Account](#)
- [Controls](#)
- [Users](#)
- [Questionnaires](#)
- [Log out](#)

Tier 2 ⌵ 10/500 + Supplier Assessments available 12 ⌵ + Assessment Demo request@suppliershield.com

Hello John McClane! Supplier chain manager


Back to assessments

16 Questions 📄 CSV

■ Not compliant

■ Partially compliant

■ Compliant



Supplier	Assessment	Evaluator	Due date	Rating
ConnectNow!	Provider security #J2XYK	Oumar Lo	-	Medium

Status Timeline

Draft
At Supplier's
In Evaluation
Completed

🔄 Repeat

Category ⌵ Evidence required ⌵ Evaluation ⌵ Criticality ⌵ Collapse all

Application security ⌵

⌵ APS-05 Evidence: no Evaluation: Compliant Criticality: high

Question text

Does your data management policies and procedures require audits to verify data input and output integrity routines?

Evidence

Compliant ⌵

Justification

Yes No Not relevant

We monthly conduct an audit.

Audit_RK63Hjv.docx ✕

Evaluator comment

Compliant ⌵ There is sufficient data to declare this control compliant.

⌵ BCR-01 Evidence: yes Evaluation: Not compliant Criticality: high

Question text

Does your organization have a plan or framework for business continuity management or disaster recovery management?

Evidence

Compliant ⌵

Justification

Yes No Not relevant

We are working on it.

Support





SUPPLIER SHIELD

<https://suppliershield.com/en>



ABILENE ADVISORS

<https://www.abileneadvisors.ch/fr/>



ABILENE ACADEMY

<https://www.abileneacademy.ch/fr/>



Rue de la Gare 39
CH - 1110 Morges



Lundi - vendredi
08:00 – 18:00



+41 21 802 35 54



+41 79 337 50 63



request@abileneadvisors.ch

