Document
C0 - Public
C1 - Interne
C2 - Restreint
C3 - Confidentiel
C4 - Secret

Forum des compétences

GT Notation et appréciation cyber des tiers

Forum des Compétences

Objectifs de l'atelier

- Etablir un état des lieux des pratiques de notation et d'appréciation cyber des tiers
- Identifier et échanger autour des problématiques liées à la construction d'un programme de notation et d'appréciation cyber des tiers
- Etablir des orientations quant à une approche commune

Structure des Ateliers

Atelier #1

Retour d'experience

Atelier #2

Objectifs et drivers du programme

(exigences des parties prenantes, exigences de conformité, KPI de succès du programme)

Atelier #3

Méthodologie du programme

(Identification des tiers à évaluer & gouvernance à déloyer en interne)

Atelier #4

Méthodologie du programme

(Approches d'appréciation à déployer pour chaque périmètre de tier identifié)

Atelier #5

Run du programme, mesure d'efficacité, amelioration

(Levier d'engagement des tiers, suivi et monitoring de l'amelioration, etc.)

Atelier #6

Mutualisation & coûts

(Opportunités de mutulisation dans l'appreciation de tiers, modèles de coûts associés avec ou sans l'utilisation de solutions externes)

Atelier #1 Retour d'expérience

Des programmes à la maturité hérérogène

Des ambitions variables en termes de périmètre d'évaluation (fournisseurs, partenaires, filiales, etc.)

Des approaches d'appréciation variées (appreciation basée sur l'autodéclaration, la revue de preuves, etc.)

Des organisation très variables (implication des achats, risques, cyber, etc.)

Des similarités observables

Les fournisseurs de service IT sont les premiers dont le risqué cyber est apprécié

Les tiers non identifiés comme critiques souvent gérés uniquement via un engagement contractuel

Un problème commun, le passage à l'échelle

Des méthodologie d'appréciation des risques peu outillées qui ne permettent pas de passer à l'échelle

Atelier #2 Objectifs et drivers du programme

Gestion des risques

Exigences de conformité

Réponses aux requêtes des clients

Ratio d'identification des tiers critiques

Ratio de tiers critiques appréciés

Niveau de performance des tiers appréciés

Niveau d'engagement des tiers dans la remédiation

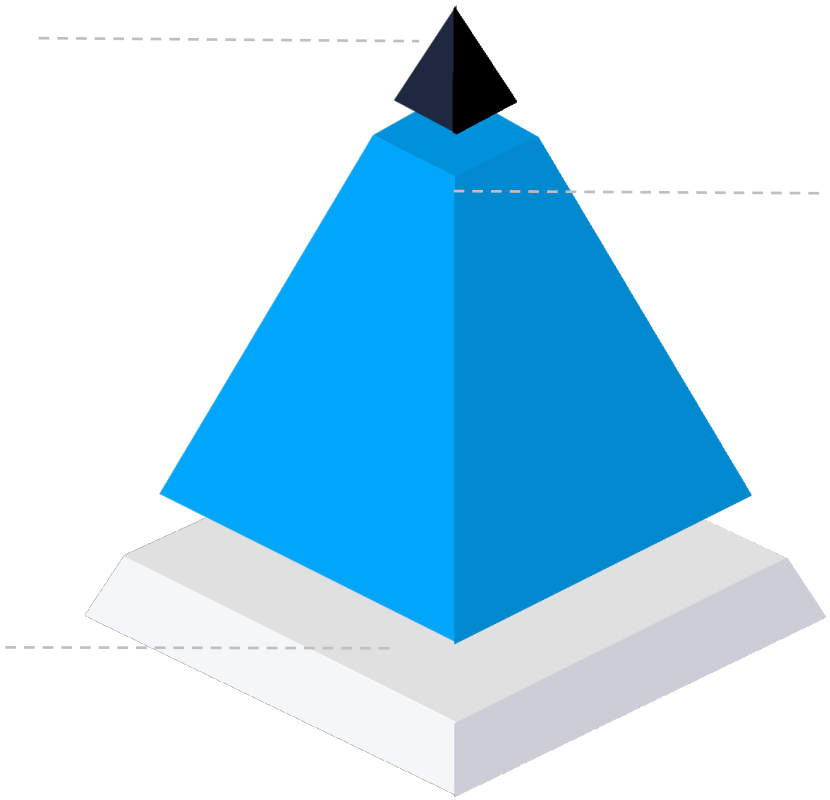
Taux d'amelioration de l'écosystème dans le temps

Atelier #3 Périmètre et organisation(2/3)

TIER 1

Prestations **critiques au sens réglementaire.**

- EBA : “Orientations relatives à l’externalisation »
- Solvabilité II
- LPM



TIER 2

Prestations critiques au sens cyber

- Données confidentielles traitées
- Accès du tier au SI et interface avec le SI du tier
- Fourniture de logiciel intégré au SI
- Criticité opérationnelle
- CA tier (> 500 k€)

TIER 3

Autres tiers, ne présentant pas les critères de criticité des tiers 1 et 2

Atelier #3 Périmètre et organisation (3/3)

Une gouvernance pour soutenir l'identification, l'appréciation et la décision d'externalisation

TIER 1

Comité d'externalisation présidé par un représentant des risques et le CISO

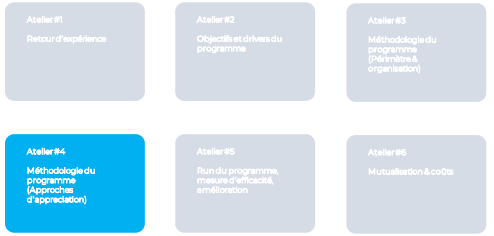
Dans ce comité, les métiers demandeurs d'externalisation présentent les risques, de plusieurs natures, liés à l'externalisation parmi lesquels le risque cyber.
Le comité définit une périodicité de ré-appréciation de chacun des risques identifiés.

TIER2

Un comité sécurité de l'externalisation, vise à identifier et se positionner vis-à-vis des fournisseurs présentant un risque cyber élevé

Il implique le CISO et un représentant des métiers concernés par l'externalisation (Business partner / Risk manager)

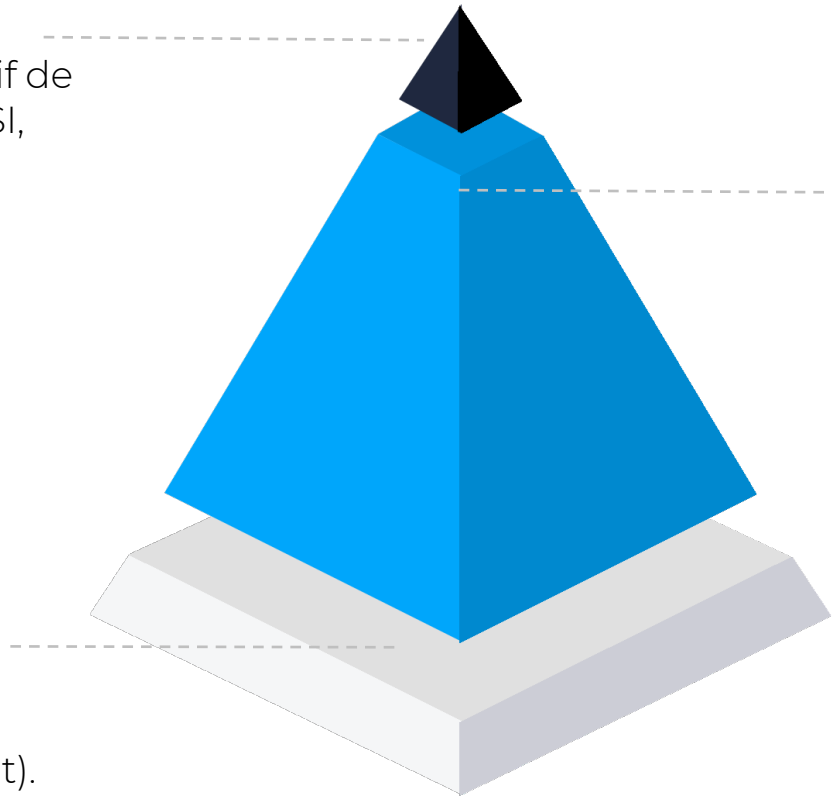
Atelier #4 Méthodologie du programme



TIER 1

Appréciation envisagée:

Contrôle de preuves sur la base du référentiel réglementaire ou normatif de l'entreprise (ex : RGPD, NIST, ISO, PSSI, PCA,...)



TIER 2

Appréciation envisagée:

Plan d'Assurance Sécurité

\+

Certification ISO 27001 / Rapport SOC 2 Type 2

Ou

Evaluation d'éléments de preuve sur les déclarations du PAS

Ou

Déclenchement clause d'audit)

TIER 3

Appréciation envisagée:

PAS simplifié (document d'engagement du tier davantage qu'un document de questionnement).

Atelier #5 Run du programme, Mesure d'efficacité, reporting et amelioration (1/2)

Identification des tiers dont on veut conduire l'amélioration

Catégorie : TIER 1 et TIER 2

Risques élevés identifiés sur la base des points de non-conformité au PAS

Tiers qui n'atteignent pas les seuils de score attendus

Identification des actions d'amélioration

Sélection des actions d'amélioration sur la base des points identifiés comme non conformes aux exigences propre à l'organisation.

NB : le choix des actions est dépendant du service rendu par le tier considéré.

Atelier #5 Run du programme, Mesure d'efficacité, reporting et amelioration (2/2)

Suivi de l'implémentation

Le role du métier est primordial dans l'engagement du tier.
Le métier doit ainsi être impliqué dans le suivi du plan d'amelioration.

la sécurité est pilote du plan d'action

le métier est pilote du plan d'action.

Leviers pour engager les tiers

Echange contradictoire pour définir un plan d'action.
L'avancement de ce plan d'action peut être évalué lors des comités de pilotage.

Annexer le PAS au contrat pour que les clauses de sorties s'appliquent en cas de manquements à la sécurité

Coûts du RUN d'un programme de gestion du risque lié aux tiers

Hypothèses

5 TIER 1 évalués par an
100 TIER 2 évalués par an

Fourchette basse :
Société mature sur la thématique : approche systématique d'évaluation pour prise de décision, population interne sensibilisée et tiers engagés. Absence d'accompagnement à la remédiation
Fourchette haute:
Société en phase de construction de l'approche : selection granulaire des tiers à évaluer, population interne à sensibiliser et tiers qui doivent être convaincus. Accompagnement renforcé à la remédiation

Périmètre	Tâche	Description	Absence d'utilisation d'outils ou de progiciel pour soutenir le processus (utilisation de spreadsheets)	Utilisation d'un solution de rating cyber équivalente en termes d'approche d'évaluation
			Coûts annuels	Coûts annuels
Global	Développement du processus d'évaluation	Maintenance des frameworks et des questionnaires, gestion du process et des outils	€	
Global	Pilotage programme	Gestion du programme, implication des parties prenantes interne	€	€
Tier 2	Engagement des tiers Revue des questionnaires et évaluation des documents Guides de remédiation des tiers Préparation des debriefs tiers	- Engagement, support, suivi, relance - Analyse et validation des documents de preuve fournis par les tiers - Revue des résultats et construction du plan de remédiation pour le tier - Elaboration de la synthèse et du benchmark du tier en vue de la réunion de debriefing	€€€€ - €€€€€	€ - €€
Tier 1	Engagement, audit de tiers critiques et remédiation	Evaluation avancée d'un tier critique (test d'efficacité, tests techniques, etc.) et remédiation	€	€
Tier 2	Collaboration avec les tiers	Réunions de débriefing, communication et suivi des plans d'ameliorations	€ - €€	€ - €€
			(€ x5 - € x8) + €	(€€ - € x5) + €

€ : Tranche de 100k€

En synthèse

- Des enjeux qui se renforcent (réglementaires et risques sécurité)
- Une nécessité de passer à l'échelle tout en déployant des methodologies d'appréciation robustes
- Une piste principale : la mutualisation de l'appréciation des tiers *(recours au partage de l'appreciation réalisée en intra groupe ou inter groupe, utilisation de solutions de scoring, etc.)*

Document
C0 - Public
C1 - Interne
C2 - Restreint
C3 - Confidentiel
C4 - Secret

Annexes

Forum des Compétences

Notation et appréciation cyber des tiers

1 – REX

- Partage des pratiques de votre entreprise

2 – Objectifs du programme

- Identification des exigences et parties prenantes et des exigences de conformité (régulateurs, clients, investisseurs, …)
- Réalisation d'un panorama réglementaire
- Définition des critères de succès du programme (Identification de tous les tiers, identification des tiers à risqué, amelioration de la maturité de l'écosystème, prise en compte de la maturité sécurité dans les achats, implication du Board, programme facilitateur de business, capacité de coordination suite à incident, …)

3 – Méthodologie du programme

- Identification des tiers à évaluer (catégories d'achat? relations? types de données? …)
- S'assurer de la participation des tiers (sourcing des tiers, action avec les tiers qui refusent de participer, action avec les tiers avec des résultats insuffisants, engagements contractuels, …)
- Choix de la méthode d'évaluation (auto-déclaratif, contrôle de preuves, Carottage / audit standards, screening technique, prise en compte de certifications, …)
- Construction des questionnaires d'évaluation (sur quels référentiels ?) / d'indicateurs techniques partageables?
- Définition de la méthodologie d'évaluation (scoring homogène, seuils acceptabilité, …)
- Définition des processus et choix des outils (appui sur des outils de rating ?)

Pour approfondir et réagir – 30" (2/2)

Notation et appréciation cyber des tiers

4 – Accompagner le changement

- Définition de la gouvernance (discussion autour de la prise en compte de l'existant)
- Intégration du programme dans l'organisation actuelle (existe-t-il une politique de sous-traitance au sein de l'entreprise ? Comment s'y inscrire ?)
- Obtenir du soutien et partager la responsabilité (soutien du board, implication des acteurs dans le changement : infosec, business et achats)
- Communiquer sur le programme (en interne, auprès des tiers, etc.)

5 – Run du programme, Mesure d'efficacité, reporting et amélioration

Au niveau du tiers (monitoring / collaboration)

- Evaluation
- Analyse des résultats et benchmark
- Définition et suivi des plans d'action (*Quelles sont les clés pour s'assurer que vos recommandations vont être prises en compte par les achats ou le business?)*
- Mesure de l'amélioration et réévaluation

Au niveau du programme :

- Prise en compte des résultats dans la cartographie des risques'

- Est-ce qu'on peut vraiment avoir un impact sur sa supply chain? Comment le mesurer?

6 – Coûts & modèle mutualisé

- La mutualisation des contrôles pour un même domaine d'activité Banque/assurance (sous quelles conditions, basée sur quel référentiel, …)
- Discussion autour du partage d'indicateurs en préventifs
- Discussion autour du partage lors de la remédiation en cas d'incident
- Discussions autour des coûts engagés lorsque l'on mène le projet in-house vs l'utilisation de solutions