QUALIFIED SECURITY ASSESSOR

Structure et optimisation des coûts de la conformité
Analyse comparée de PCI DSS et ISO 27001

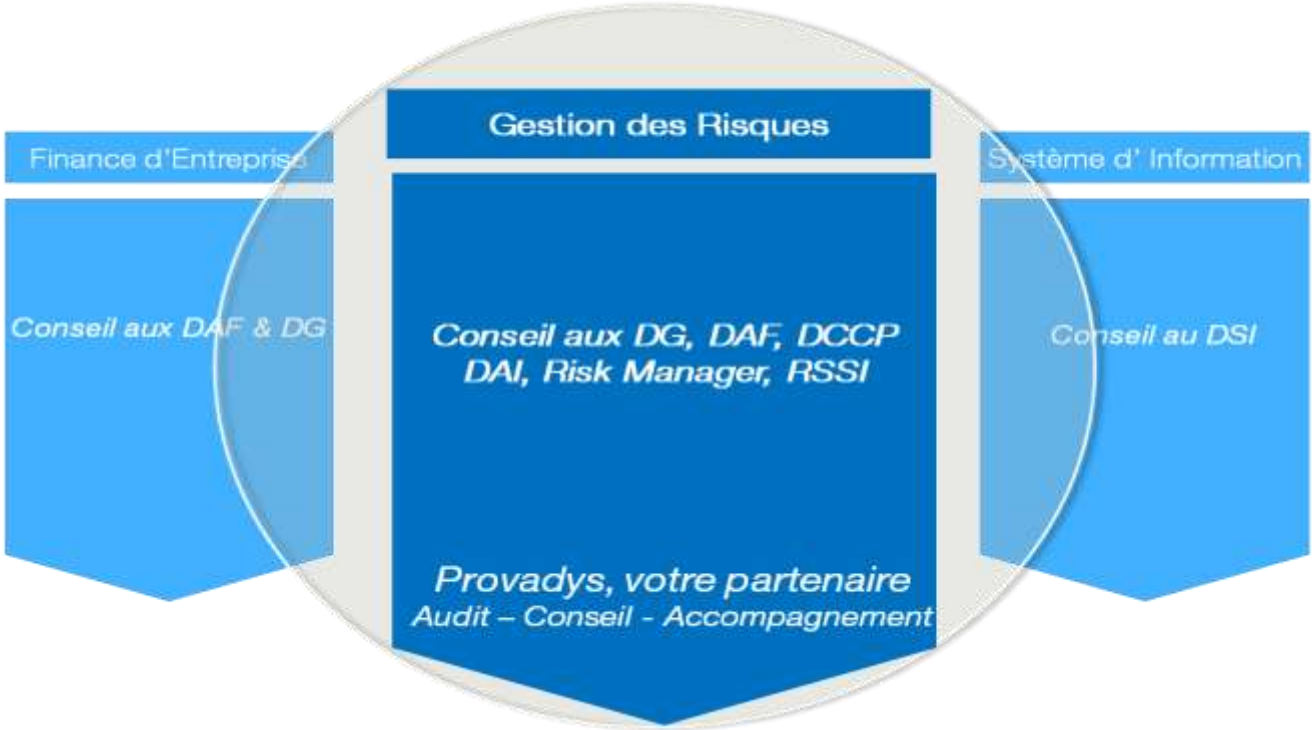
CNIS EVENT

27 avril 2011

Paris

Services à Haute Valeur Ajoutée

Provadys est un cabinet d'audit et de conseil spécialisé sur trois domaines d'activités spécifiques : La Finance d'Entreprise, La Gestion des Risques et Les Systèmes d'Information

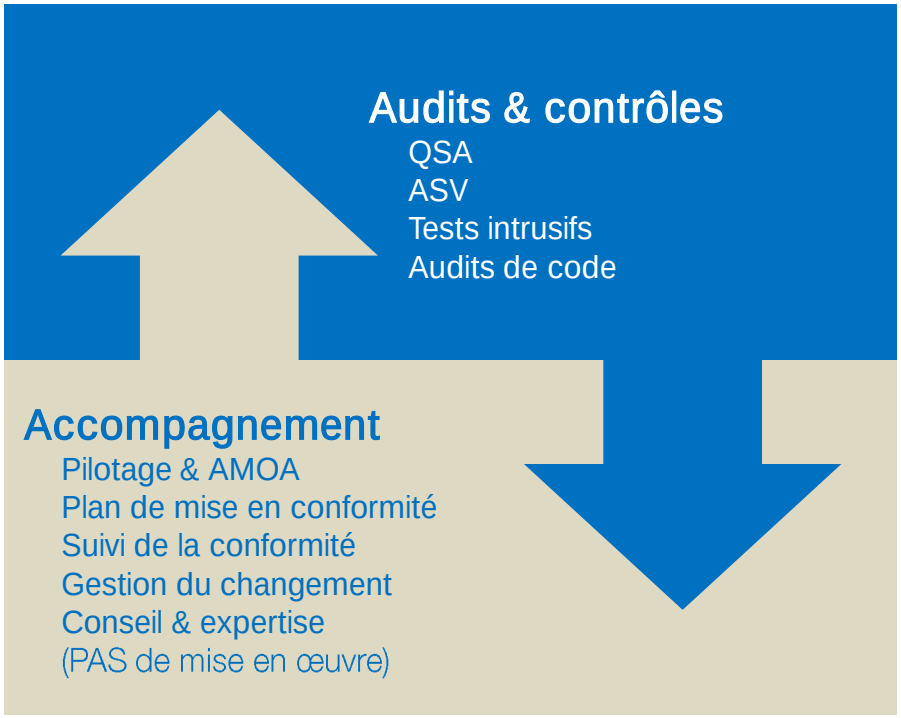


L'offre Gestion des Risques regroupe à la fois les compétences de profils ayant une expertise métier et des profils ayant une expertise technique.

Cette double compétence permet à Provadys d'intervenir de manière transversale sur les missions en intégrant les enjeux métiers mais aussi techniques.

Provadys est certifié *QSA Company*, ce qui lui permet de se positionner en tant qu'entité habilitée à réaliser les audits certifiants PCI QSA

Une offre de service complète en toute déontologie :



PCI Security Standards Council
QUALIFIED SECURITY ASSESSOR

Provadys est référencé par le GIE Cartes Bancaires, garantie d'une offre en langue française, adaptée au marché "CB" ainsi de la confidentialité totale des données recueillies pendant ces audits.

Structure et optimisation du coût de la conformité

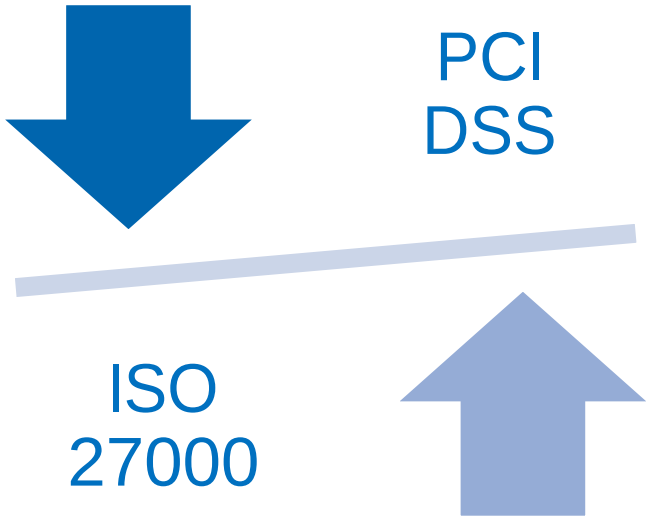
Introduction

Les objectifs de la présentation

Analyse comparée de PCI DSS et ISO 27001 à travers l'approche par les coûts

Des normes aux multiples points communs mais tellement différentes

- PCI DSS et les normes de la famille ISO 27000 sont rarement approchées à travers la dimension des coûts
- L'objectif de la présentation est de poser quelques éléments de comparaison des deux modèles de coûts et des possibilités d'optimisation
- Le contenu des deux normes n'est pas abordé
- Il ne s'agit pas d'élire la « **meilleure norme** »



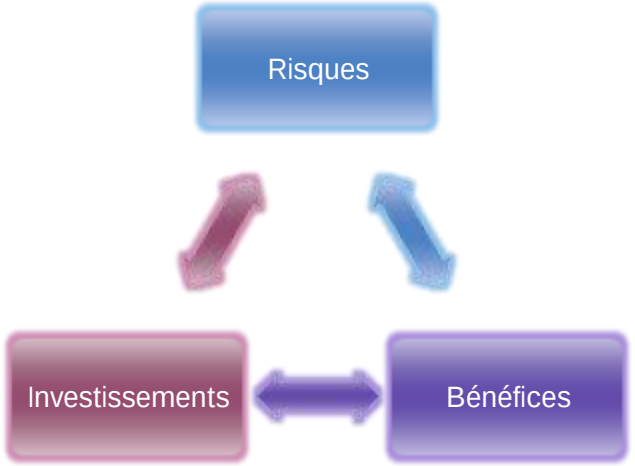
PCI DSS et ISO 27001

Une approche par les coûts

Des points communs et des questions qui fâchent

Il est difficile de savoir se prononcer 'a priori' sur le ROI de PCI DSS

- PCI DSS n'est pas une NORME ou un texte de loi mais un ensemble de mesures visant à traiter le risque de divulgation massive de données Cartes Bancaires
  - Les entreprises commerciales se posent légitimement la question de l'intérêt économique de se mettre en conformité
    - »Qu'avons-nous à y gagner ?
    - »Les investissements seront-ils compensés / dépassés par les gains ?
  - L'approche Investissement vs Bénéfices doit être corrigée par la prise en considération des risques
    - »Que risque-ton de perdre si nous n'y allons pas ?
    - »Les risques seront-ils ramenés à un niveau acceptable ?



Des points communs et des questions qui fâchent

Il est difficile d'envisager une démarche ISO 27001 sous l'angle ROI

- ISO 27001 est une norme aussi « facultative » que ISO 9001
  - L'utilisation de la famille 27xxx comme référentiel de bonnes pratiques pour la SSI s'impose comme une évidence
  - La certification fait encore débat
    - »A quoi bon puisque le travail est déjà fait ou sera fait de toutes façons ?
    - »A quoi bon puisque cela ne garantit pas que le SI est mieux sécurisé ?
- La démarche de certification ISO 27001 relève le plus souvent d'une volonté stratégique
  - Les questions économiques sont souvent au second plan
  - Il s'agit le plus souvent de pérenniser le travail réalisé dans la mise en place des bonnes pratiques
  - La certification est vue comme un outil de valorisation et de génération de nouvelles opportunités

Des points communs et des questions qui fâchent

Il est difficile de savoir ‘a priori’ combien va couter la conformité à PCI DSS

- En première analyse les coûts associés ne sont pas négligeables
- Les éventuels gains sont a priori très dépendants des activités
- Les investissements sont dépendants de la situation de départ de chaque entité
- Le marché français est très peu mature
  - Peu d’entreprises certifiées
  - Peu d’acteurs de référence

  ==> Pas de benchmark fiable
- Il persiste des zones de flou
  - Pénalités
  - Échéances

COMBIEN ??? Sur COMBIEN de temps ???

Des points communs et des questions qui fâchent

Il est difficile de savoir 'a priori' combien va couter la conformité ISO27001

- L'appréciation intuitive des coûts est souvent fausse
- De nombreux facteurs doivent être pris en compte
  - Périmètre
  - Analyse de risques
  - Mesures retenues dans le SOA
  - Ecarts initiaux
- Le marché français pour ce qui est de la mise en conformité et certification ISO 27001 est beaucoup plus mature
  - Plusieurs acteurs de référence
  - Des ébauches de benchmark dans certains secteurs d'activité

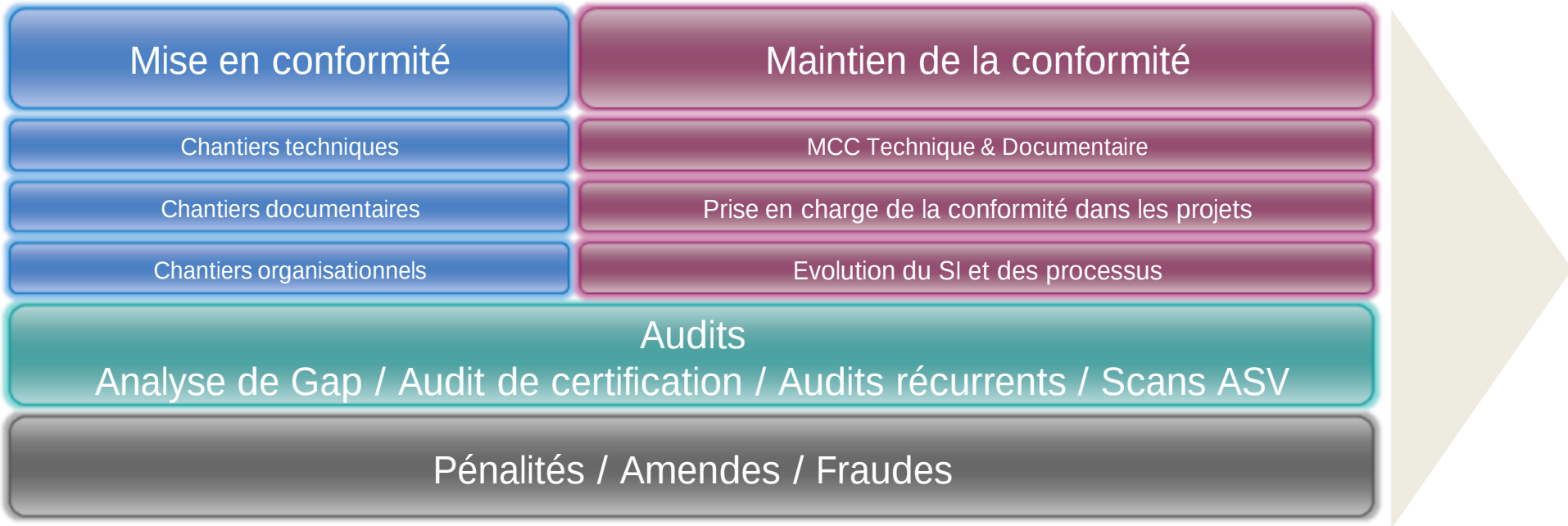
Modèles et optimisation

Comparaison des modèles

Comment appréhender le coût de la conformité PCI DSS

Se mettre en conformité PCI DSS et le demeurer peut couter cher

- Au-delà du constat, il est souvent difficile de donner une vue complète des coûts associés à la conformité PCI DSS
- Plusieurs axes se dégagent



Comment appréhender le coût de la conformité ISO 27001

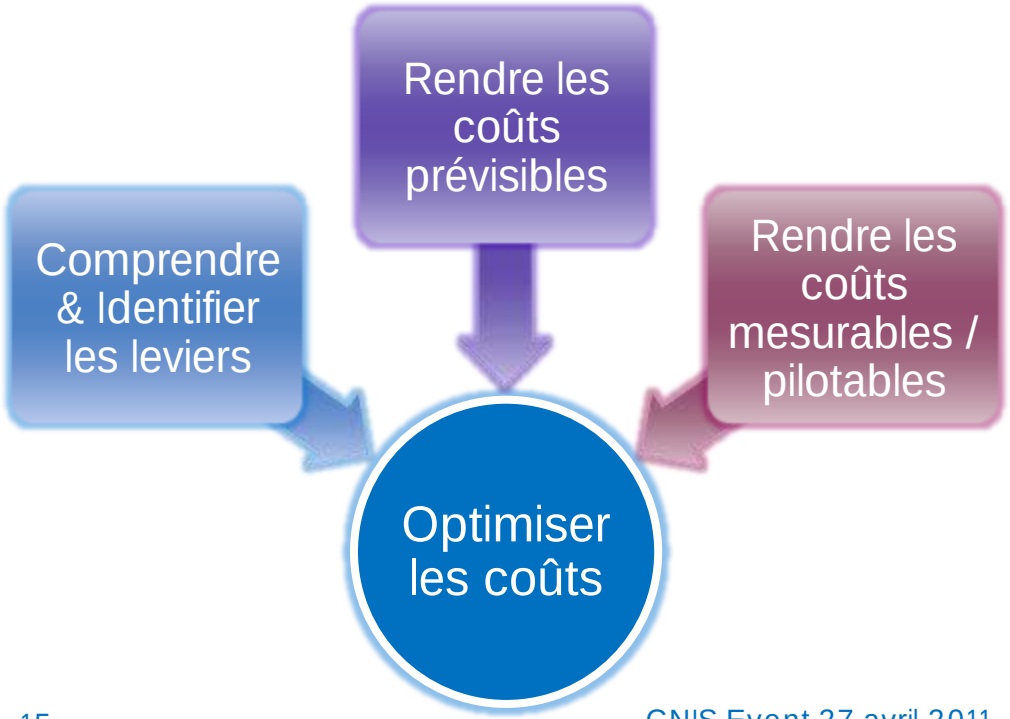
Les grands axes de la structure de coût sont très similaires

- Peu de zones d'incertitude
- Les pénalités n'ont de sens que si la conformité ISO 27001 est intégrée comme un engagement contractuel

Amener les coûts au niveau optimal en agissant sur les différentes briques de la structure de coûts

Optimiser les coûts ne signifie pas seulement les réduire

- Les objectifs
  - Comprendre les coûts et identifier les leviers
  - Rendre les coûts prévisibles
  - Rendre les coûts mesurables
  - Rendre possible la gouvernance
- Adapter les coûts aux objectifs
- Maximiser les ratio
  - Bénéfices / Investissement
  - Risques / Investissement
  - Opportunités générées / Investissement



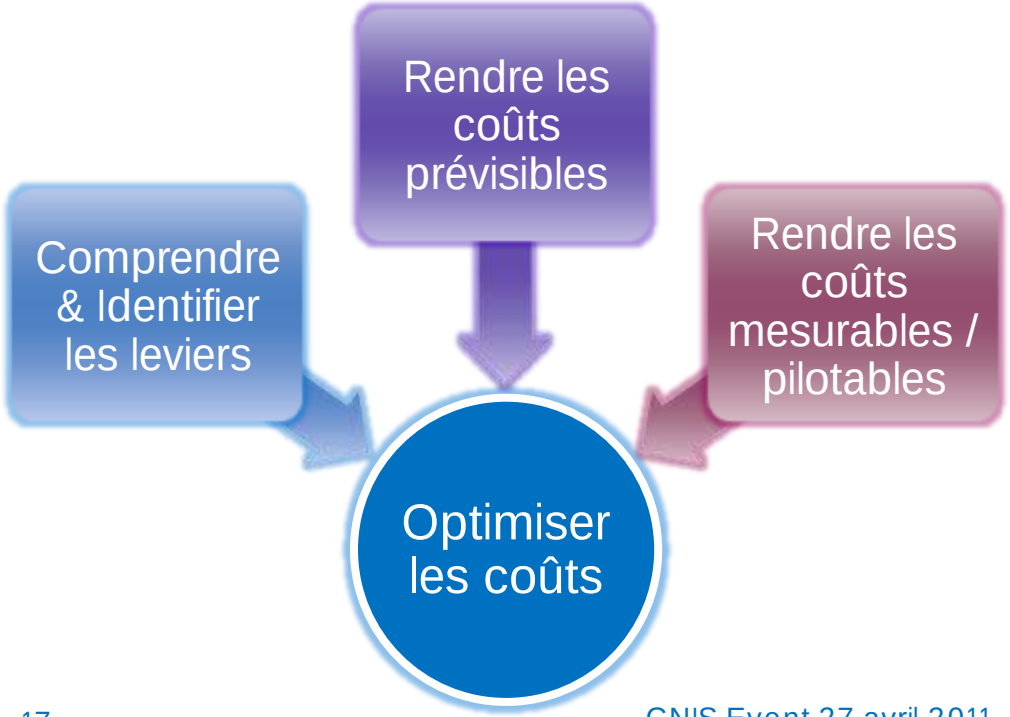
L'optimisation des coûts

*Présentation de l'approche **Provadys** de l'optimisation des coûts*

Les principaux axes communs de l'optimisation des coûts

Application de la structuration des coûts

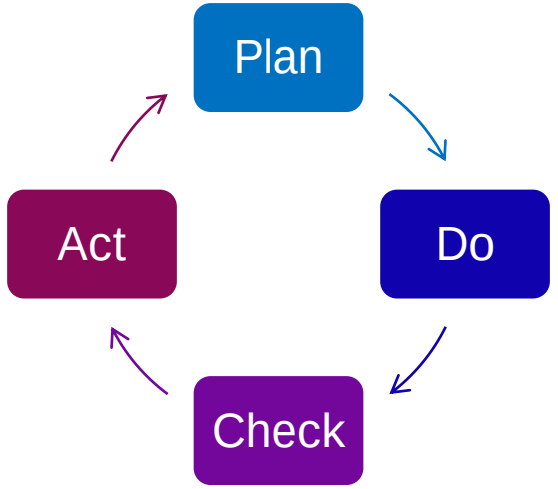
- A partir de l'analyse de gap identifier les leviers dans chaque chantier
  - Réduction des risques
  - Réduction des dépenses
  - Limitation des dépenses prévisibles
  - Caper les coûts non prévisibles
- Traquer les inconnues, réduire les incertitudes
- Capex, Opex, Coûts de transformation
  - Chantiers techniques
  - Conduite du changement
  - Process Reengineering
- Mise en place des KPI (indicateurs)
- Tableaux de bord et outils de gouvernance



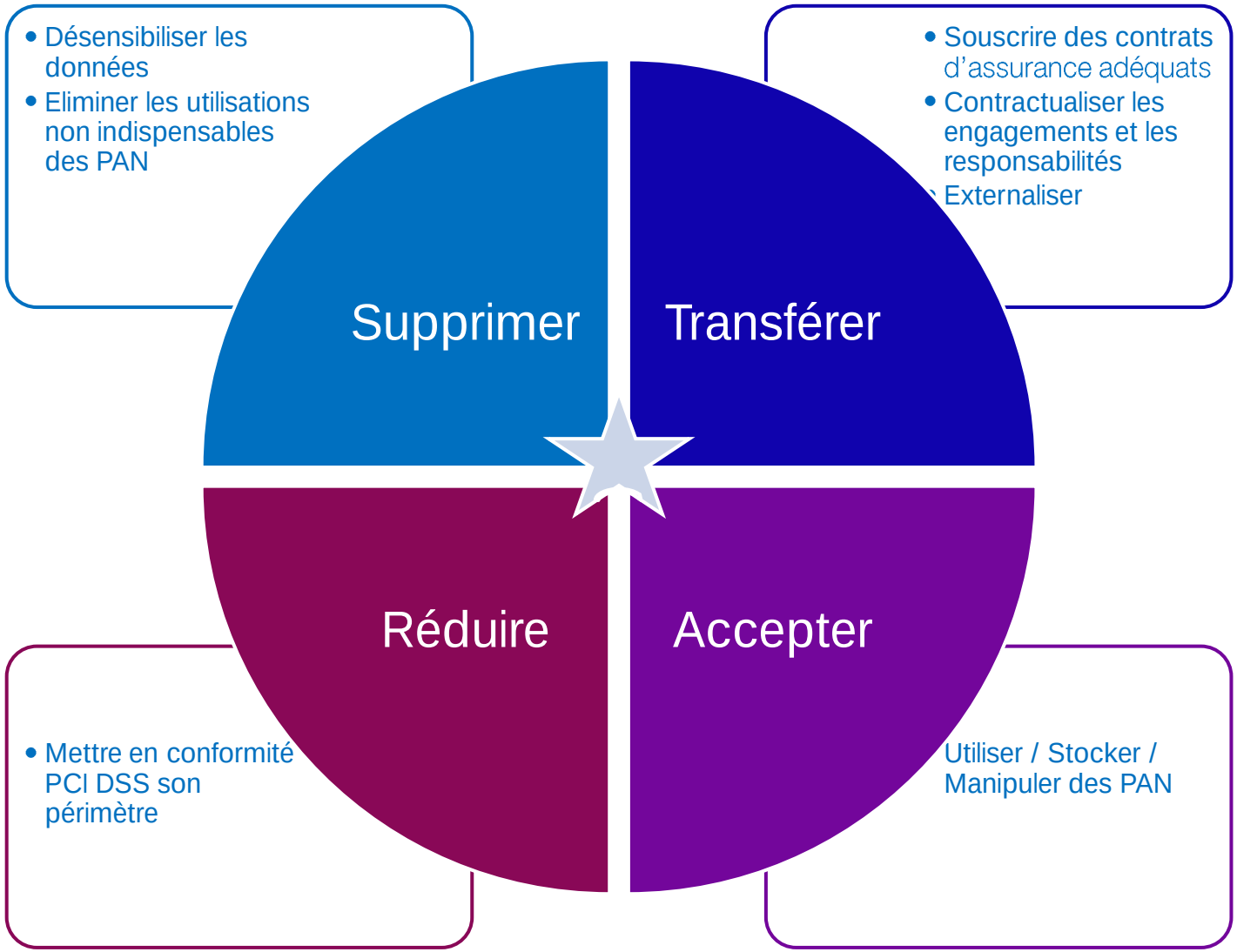
Ne pas séparer la mise en conformité du maintien de la conformité

Du programme de mise en conformité au Système de Management de la Conformité

- La certification n'est pas la fin mais seulement un début
- La mise en conformité n'est pas un projet menant à la certification
- Chaque brique du programme doit initier les processus sur lesquels reposera le maintien de la conformité
- Le programme de mise en conformité doit donner vie aux processus de maintien de la conformité
- Le programme de mise en conformité doit être vu comme un programme de transformation durable
- Tous les investissements doivent être examinés à la lumière de l'application de ce cycle



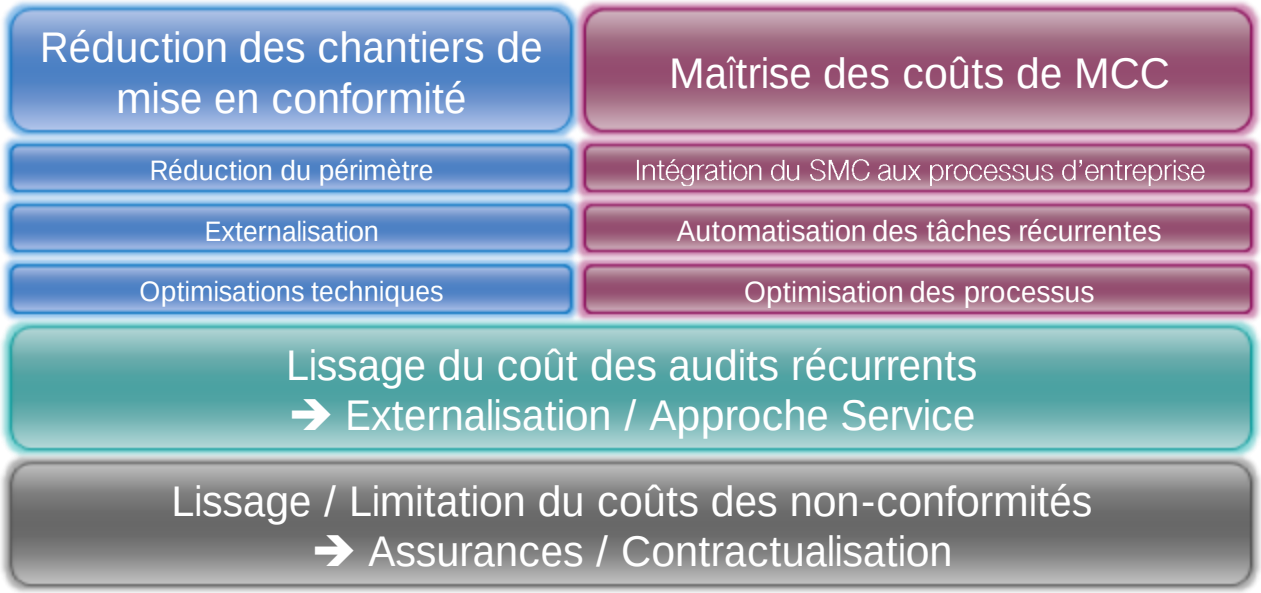
Envisager les multiples réponses possibles face au traitement des risques associés aux données Cartes Bancaires



Les principaux axes de l'optimisation des coûts

Il est possible d'agir sur toutes les briques de la structure de coûts

- Réduction du périmètre
  - Segmentation réseau
  - Désensibilisation des données
    - Chiffrement
    - Tokenisation
  - Externalisation
  - Monétique centralisée
- Transfert de responsabilités
  - Contractualisation
- Transfert de risques
  - Assurance



Les principaux axes de l'optimisation des coûts

Il est possible d'agir sur toutes les briques de la structure de coûts

- Réduction du périmètre
  - Choisir le bon périmètre pour pouvoir communiquer et valoriser la certification
  - Soigner l'analyse de risques pour s'aligner avec la stratégie d'entreprise et les gains SSI visés
  - Choisir les bonnes mesures dans le SOA
  - Planifier avec soin la mise en conformité
- Transfert de responsabilités
  - Contractualisation
- Transfert de risques
  - Assurance

Conclusions

Ce qu'il faut retenir et pour aller plus loin

Les programmes de conformité aux normes PCI DSS et ISO 27001 ont des modèles de coûts proches mais disposent de leviers d'optimisation différents

Les optimisations de coût sont possibles

- ISO 27001 intègre plus de liberté pour l'optimisation des coûts
  - Périmètre
  - Objectifs
  - Planning
- PCI DSS est beaucoup plus contraignante
  - Le choix du périmètre n'est pas libre
  - Réduire le périmètre demande des efforts
  - Les exigences de conformité sont plus directives

- L'optimisation des coûts dans la mise en conformité est une réflexion indispensable et un facteur clé de succès pour ces programmes.

Questions / Réponses

Rendez vous à la pause

Finance d'Entreprise

Gestion des Risques

Systèmes d'Information

▪ audit ▪ conseil ▪ accompagnement ▪ provadys.com

Contact : Luc DELPHA

01 46 99 93 80

Provadys