GS Days
LES JOURNÉES FRANCOPHONES DE LA SÉCURITÉ
2016

POLITIQUES DE SÉCURITÉ INAPPLICABLES…
ET INAPPLIQUÉES!!
COMMENT FAIRE MIEUX?

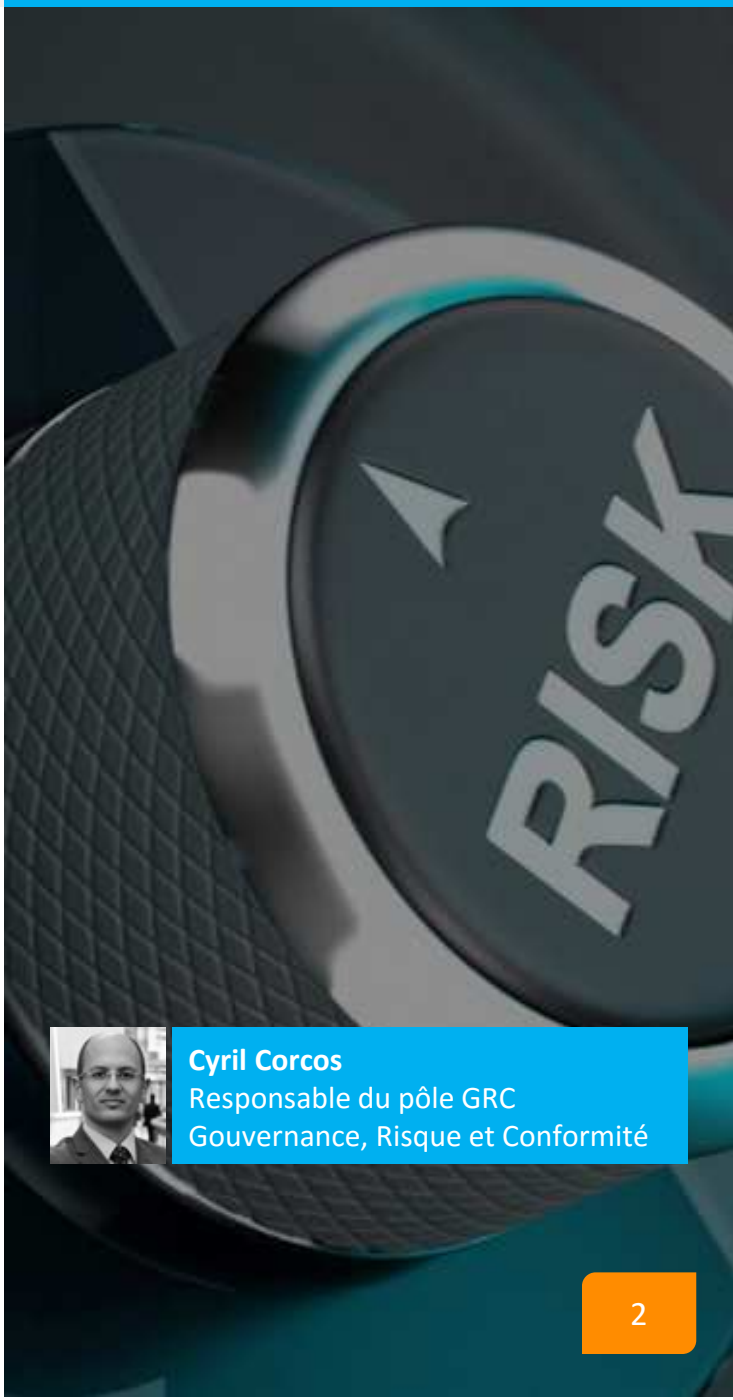
harmonie

07/04/2016

Agenda

GOVERNANCE,
RISK & COMPLIANCE

1. Présentation de Harmonie Technologie
2. Contexte
   - Introduction
   - Pourquoi fait on des politiques de sécurité?
3. Morceaux choisis de politiques inapplicables… et inappliquées
4. DO / DO NOT
5. Questions / Réponses



Cyril Corcos
Responsable du pôle GRC
Gouvernance, Risque et Conformité

PRÉSENTATION DE HARMONIE TECHNOLOGIE

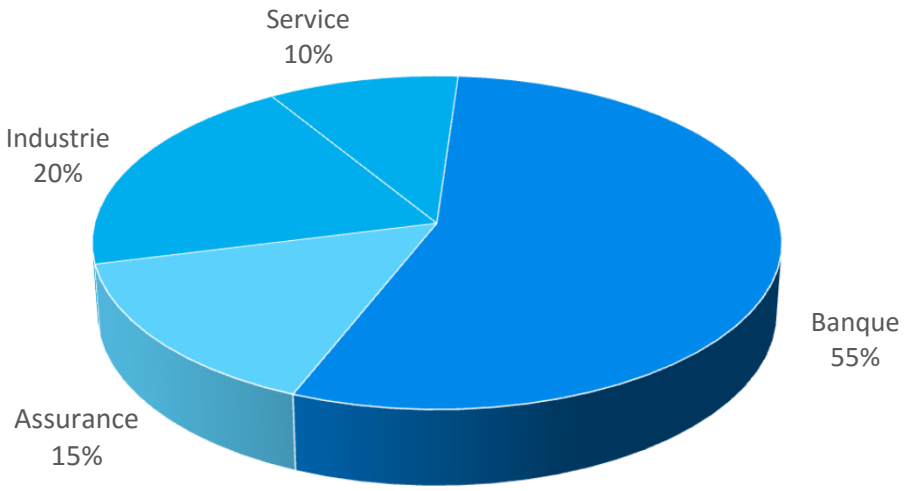
harmonie

Partenaires sécurité des grandes entreprises

Cabinet de Conseil - Spécialiste Risk Management & Sécurité SI

- AUDIT
- CONSEIL
- INTÉGRATION
- FORMATION

Une Clientèle grands comptes



HARMONIE
2005-2016

CHIFFRES CLES

Croissance organique soutenue depuis 2005 de 30% par an

2015
85 collaborateurs et 9,3 M€ de CA

Projection 2016
+ de 100 collaborateurs et 12 M€ de CA

EVENEMENTS

Spécialiste Risk Management & Sécurité SI

GOVERNANCE, RISK & COMPLIANCE	« Organiser et piloter la SSI »
IDENTITY & ACCESS MANAGEMENT	« Maîtriser les habilitations et accès au SI »
DATA PROTECTION & PRIVACY	« Protéger son patrimoine Informationnel »
CYBER SECURITY	« Auditer et surveiller la sécurité du SI »

UNE **APPROCHE TRANSVERSE DE LA SSI** AU SERVICE DES INNOVATIONS D'ENTREPRISE.

- Mobilité et télétravail
- Transformation digitale
- Externalisation des services dans le cloud
- Digitalisation de la relation client
- Objets connectés

\+ Un cabinet de conseil **INDEPENDANT** en Risk Management et SSI

\+ Une **COMPLEMENTARITE** des compétences :
- Organisationnelle
- Fonctionnelle
- Technique
- Audit

\+ Plus de **10 ANS D'EXPERIENCE** en SSI

Vos interlocuteurs

Sophie Grynszpan
Directrice du développement

Jennifer Bellagamba
Manager commercial

Cyril Corcos
Partner GRC

Thomas Jolivet
Partner IAM

Christophe Gueguen
Partner DATA & CYBER SECURITY

Siège social : 60 rue la Boétie Paris 8.

Std. +331 73 54 30 00
Fax +331 73 54 30 01

Site : www.harmonie-technologie.com
Linkedin : www.linkedin.com/company/harmonie-technologie
Twitter : www.twitter.com/HarmonieSSI

POLITIQUES INAPPLICABLES… ET INAPPLIQUÉES

harmonie

Introduction

Le mieux est l'ennemi du bien.

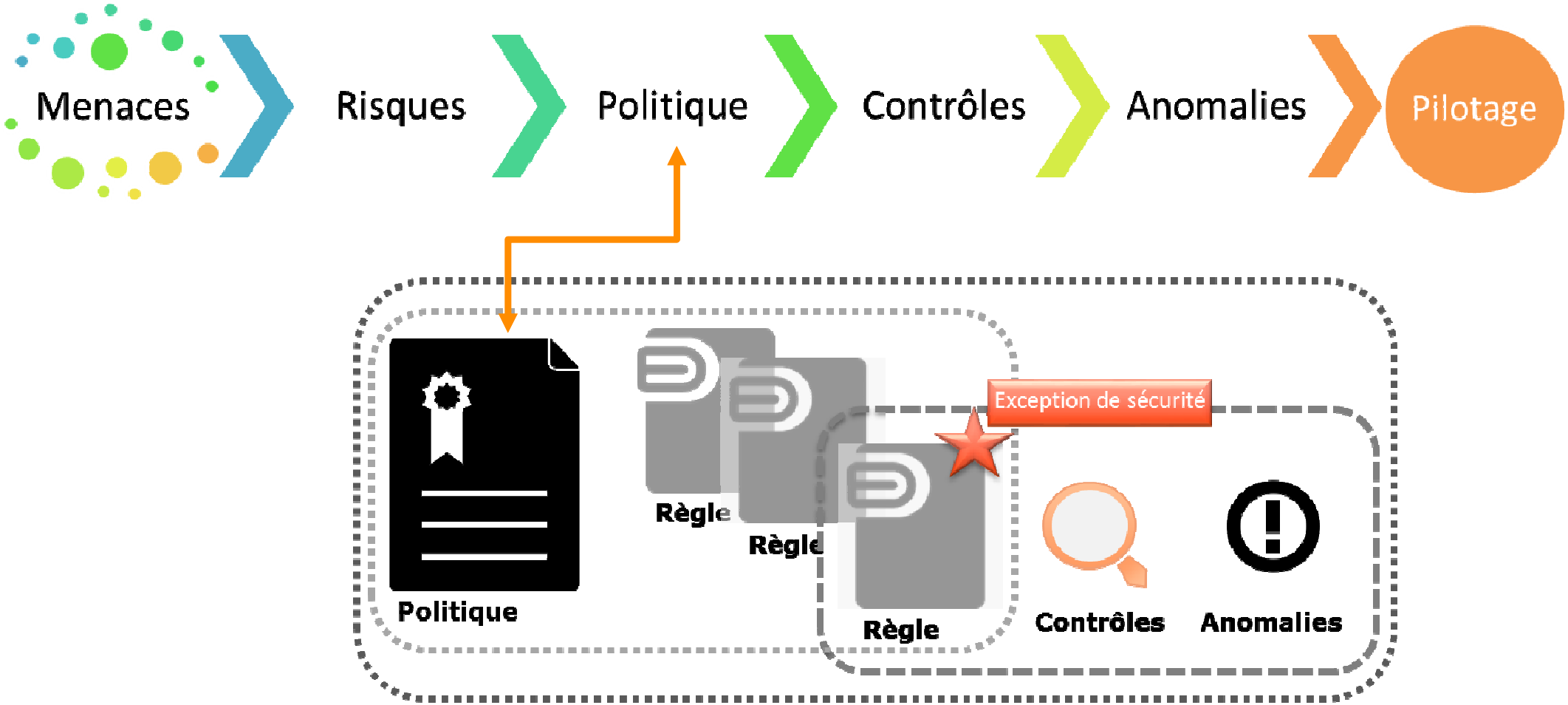
Ce vieil adage trouve une résonnance particulière dans les politiques de sécurité où les **règles les plus vertueuses** rivalisent toujours plus d'**infaisabilité**.

Nous vivons à une époque où les menaces se concrétisent régulièrement en incidents de sécurité et où les **politiques de sécurité**, pour être efficaces, doivent être **cohérentes avec les moyens** dont disposent les RSSI.

Les commandements bibliques du « **besoin d'en connaître** » et du « **moindre privilège** » nécessitent ils d'être adaptés à l'ère de la transformation digitale, de la cybercriminalité et du cloud ?

Pourquoi fait on des politiques de sécurité?

Une politique de sécurité est un ensemble de règles qu'un groupement d'intérêts communs se donne pour répondre - d'une certaine manière - à des menaces



Pourquoi fait on des politiques de sécurité?

Une politique de sécurité peut avoir plusieurs finalités:

- Définir le cadre de référence quant au fonctionnement de l'entreprise
  - En définissant des seuils
  - En faisant la promotion de cibles, via des trajectoires
- Démontrer la volonté de l'entreprise de respecter les règlementations / bonnes pratiques de place

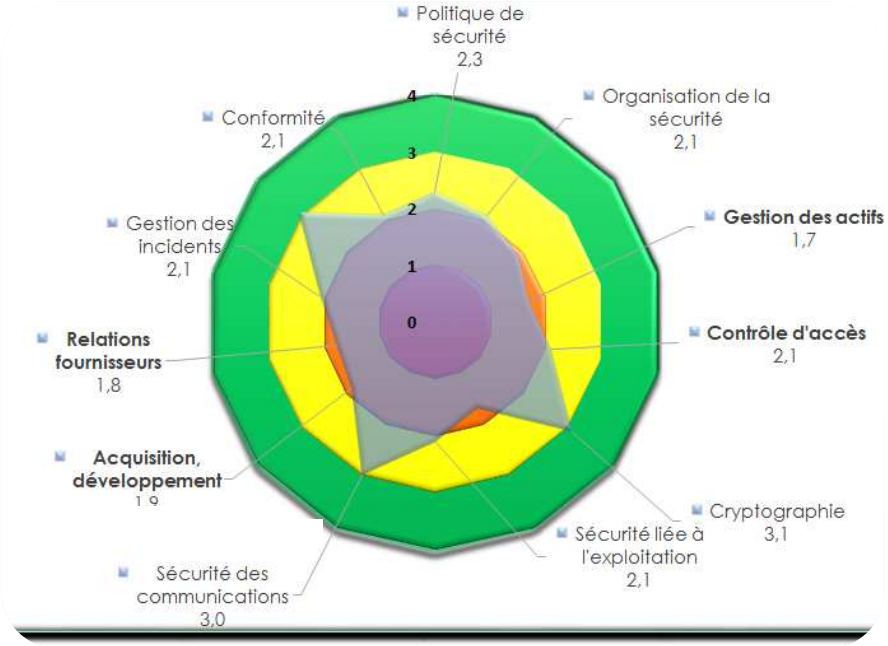
Comment une politique peut elle être - ou devenir - inapplicable?

- Constituer une marche beaucoup trop haute
- Nécessiter des moyens/investissements non-disponibles
- Etre associée à des délais de mise en œuvre trop court
- Etre liée à des processus et/ou solutions inefficaces

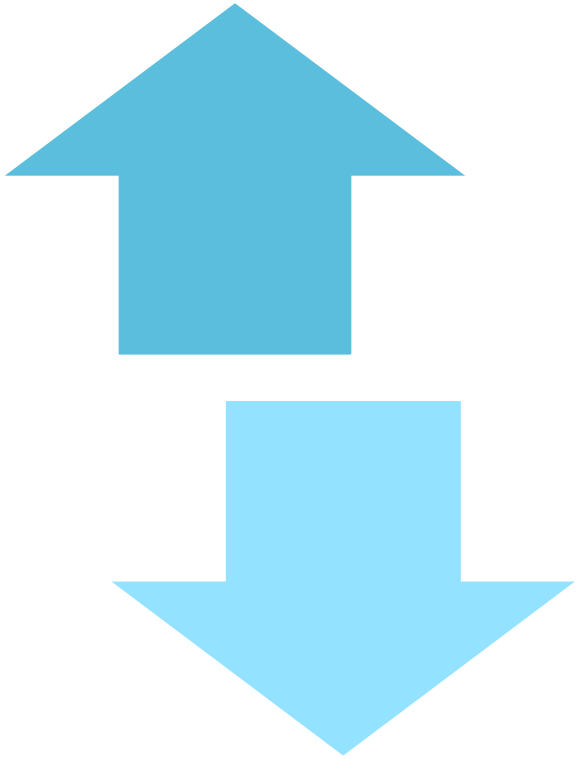
Une politique est un consensus sur une ambition à un instant donné

Des exemples de politiques particulières, choisies sur la base des catégories ISO2700n:

- Gestion des actifs
- Contrôle d'accès
- Acquisition et développement



Protection de l'information



La plupart des échelles de classification de l'information s'appuie principalement sur l'appréciation d'un critère essentiel, l'impact de divulgation de l'information

Exemples:

- « A un impact irrémédiable sur .. »,
- « génère une perturbation », « significative », « contournable », « non bloquante »
- « pourrait nuire à un projet, une activité »

Mais à la lecture de ces impacts potentiels:

- Les utilisateurs finaux comprennent-ils concrètement de quoi il s'agit et qualifient-ils l'information à bon escient ?
- Quid de l'utilisation des données de production durant les projets? Quid de l'anonymisation? Des extractions massives sauvages?

#principescompris
#bonneapplication
#donnerlesoutils

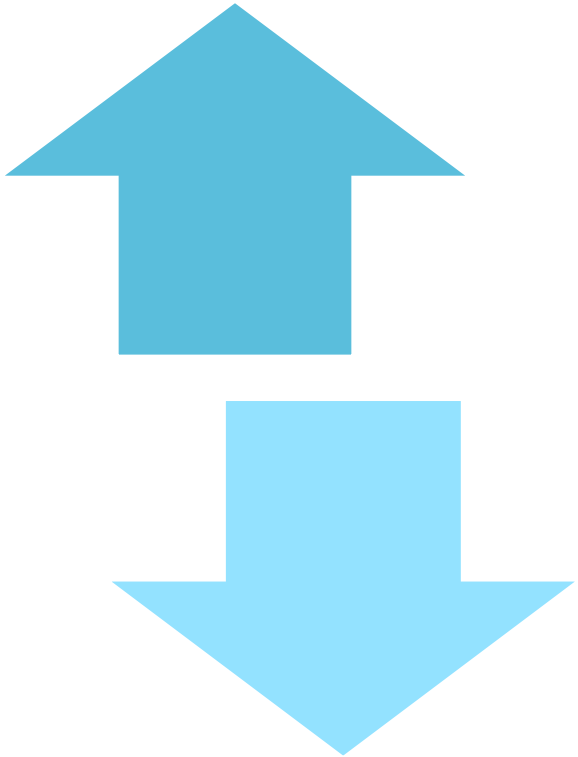
Au final, la classification d'une information est souvent:

- Considérée uniquement sous l'angle du nombre des personnes auxquelles elle peut être diffusée
- Héritée du « container » qui stockait la précédente information

Protection de l'information

Qu'ont ils changé depuis, pour mieux gérer l'impact de l'éventuelle divulgation de leurs informations? Pourquoi ne pas l'avoir fait avant?

Contrôle d'accès



Les principes

- Le Responsable d'un collaborateur est responsable de tout:
  - Valider l'attribution d'accès
  - Garantir que tous les accès sont justifiés, les revoir régulièrement, certifier leur pertinence
  - Identifier des accès permettant de réaliser des opérations frauduleuses
  - Etc.

La réalité

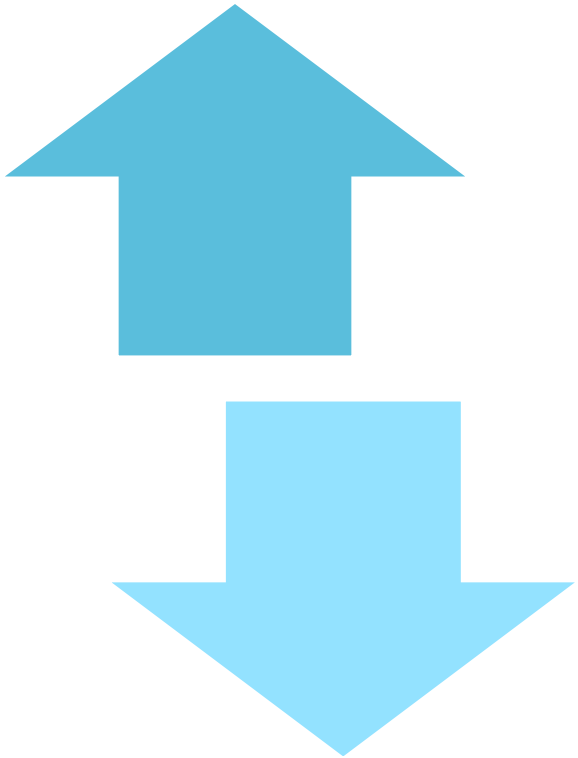
- Donne-t-on aux Managers l'information nécessaire leur permettant de faire ce travail:
  - La liste de tous les accès existant de leurs collaborateurs
  - La signification des applications et des droits permettant:
    - De comprendre ce qui est demandé
    - De s'assurer de la compréhension de ce qui est (re)certifié
  - Des outils facilitant la réalisation de ces opérations
  - Un nombre raisonnable de demandes

#donnerlesoutils
#donnerdusens

Au final, quelle confiance accorder réellement aux dispositifs (processus et solutions) en place?

Acquisition et développement

Rappel du contenu de cette catégorie selon ISO27k: Intégrer la sécurité dans le cycle de vie du projet et protéger les données de test



La gouvernance de la gestion des risques est au centre de cet exercice

- Les projets, en tant que changements, induisent des risques dont les fonctions support (DSI, Risques, Conformité) ne sont que les gestionnaires, pas les propriétaires
- Le RACI des politiques de sécurité requièrent souvent des lignes métiers :
  - Qu'elles soient propriétaires de leurs systèmes d'information
  - Qu'elles assument (revoient / arbitrent) leurs risques et traitent leurs plans d'action

La réalité

- Quelle proportion de projets réalise une analyse de risque? Combien, avec une granularité adaptée aux enjeux?
- Les risques sont ils suivis durant le projet?
- Comment sont réalisés les arbitrages? Qui prend la décision?
- Comment sont suivis et consolidés les risques acceptés?

#rolesassumes
#donnerdusens

Au final, est ce que les risques projets sont réellement maîtrisés?

Propositions permettant simplement d'arriver à des résultats tangibles

DO

- Déterminer la contribution d'une règle à la couverture des risques de l'entreprise et définir des seuils de qualification
- Faire une analyse d'impact 360° des coûts et délais de l'application d'une nouvelle règle, afin d'en vérifier l'applicabilité concrète au regard des budgets
- Prévoir une feuille de route d'application de la règle, avant que celle-ci ne devienne opposable
- Aligner si possible/opportun les rythmes de modification des politiques de sécurité avec les exercices budgétaires et les plans d'audit
- Reconsidérer les règles d'entreprise pour déterminer si une règle partielle n'existe pas déjà

DO NOT

- Ne pas établir de règles sans prévoir les solutions pratiques et ergonomiques
- Ne pas exclure la possibilité d'exception. L'exception n'est pas la règle, mais la règle donne son sens à l'exception
- Eviter la création de rôles spécifiques pour une politique particulière
- Ne pas se préoccuper des délégations
- Ne pas renoncer à supprimer des règles


SUCCESS
IDEA
PRODUCTION
PRODUCT
RESULT
SUCCESS
PROCCESS
TEAM
COMMUNITY
GROUP
MEDIA
WEB
IDEA
WORKSTATION
WORK GROUP
STORAGE
SERVER

harmonie