



GRIFES

# Gestion des risques et au-delà

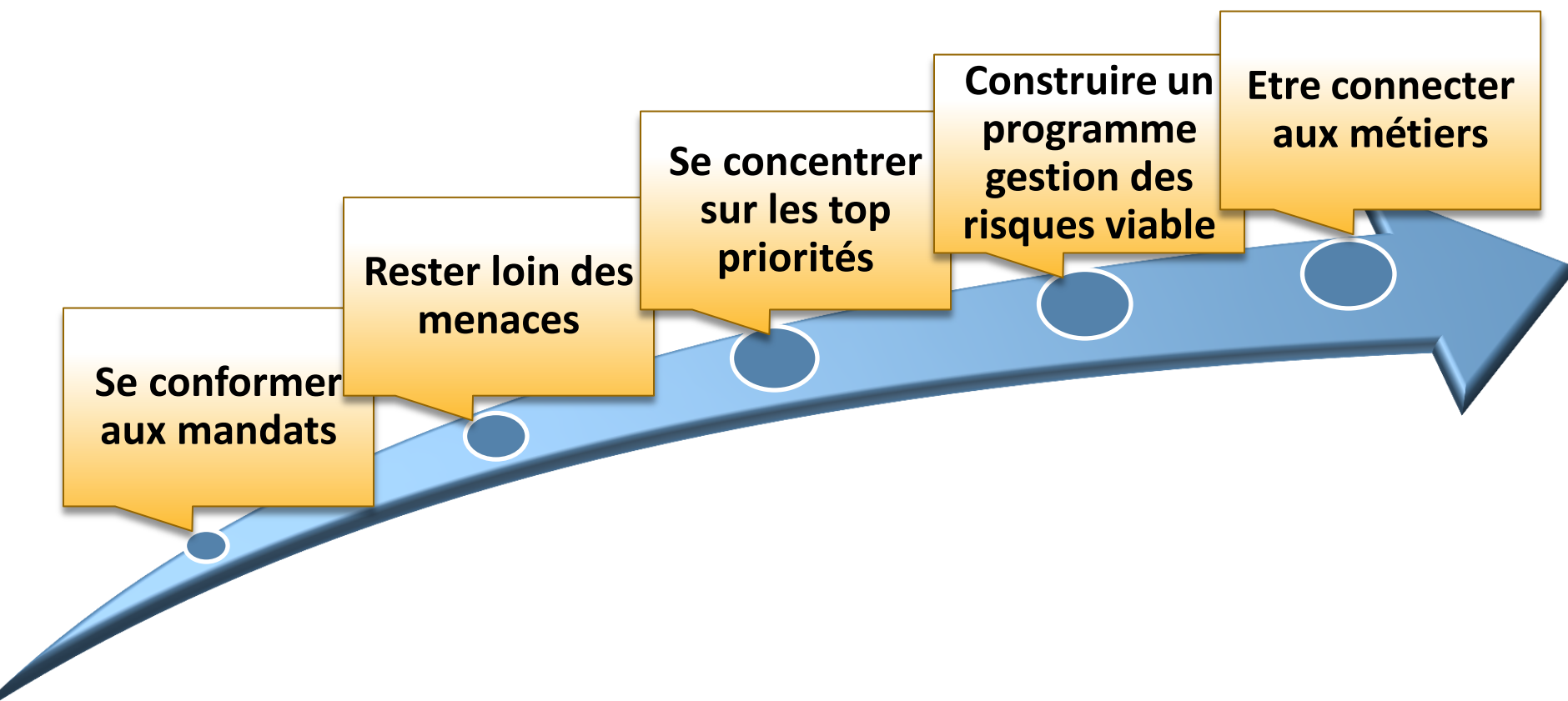
**Pablo C. Martinez**

TRMG Product Leader, EMEA

Symantec Corporation



# Gestion des risques et conformité – Principaux soucis



# De la conformité à la gestion du risque métier

**Se conformer  
aux mandats**

**Rester loin des  
menaces**

**Se concentrer  
sur les top  
priorités**

**Construire un  
programme  
gestion des  
risques viable**

**Etre connecter  
aux métiers**

**Les entreprises suivent, en  
moyenne, 17 standards ou  
normes.**

**36% d'entre elles les gèrent sur  
tableur ou manuellement.**

*Source: Symantec 2010 State of the  
Enterprise Security Report*



# De la conformité à la gestion du risque métier

Se conformer  
aux mandats

**Rester loin des  
menaces**

Se concentrer  
sur les top  
priorités

Construire un  
programme  
gestion des  
risques viable

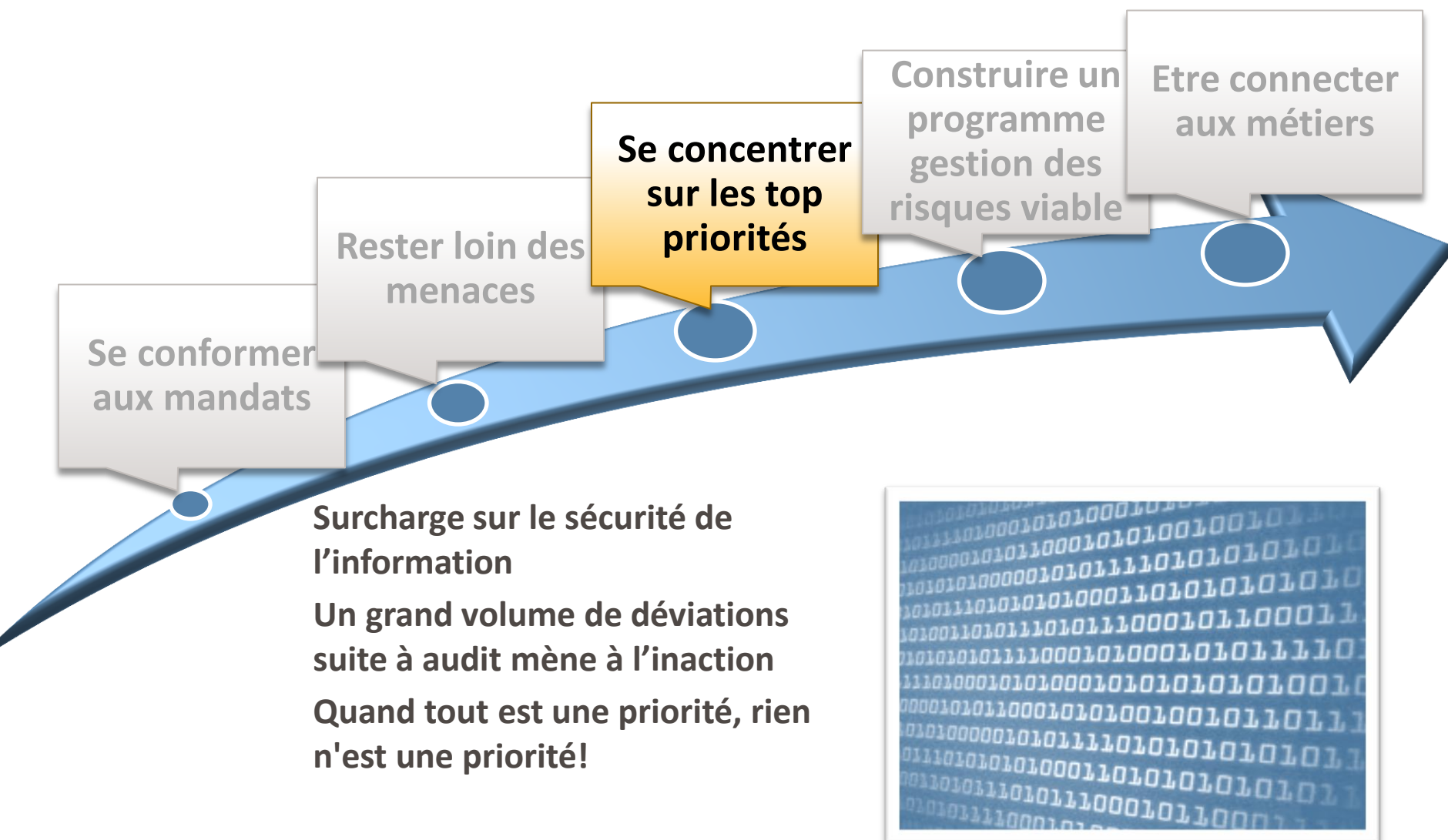
Etre connecter  
aux métiers

*“98% des incidents (sur les données) auraient pu être évité par des mesures simple ou intermédiaires”*

*Source: Verizon Data Breach Investigations Report, 2012*



# De la conformité à la gestion du risque métier



# De la conformité à la gestion du risque métier

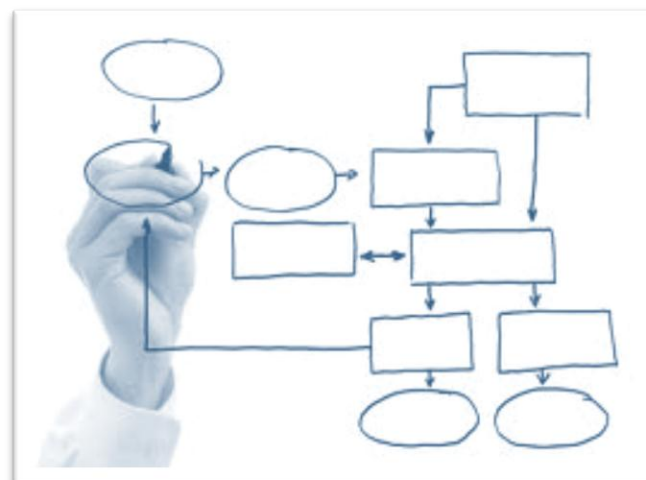
Se conformer  
aux mandats

Rester loin des  
menaces

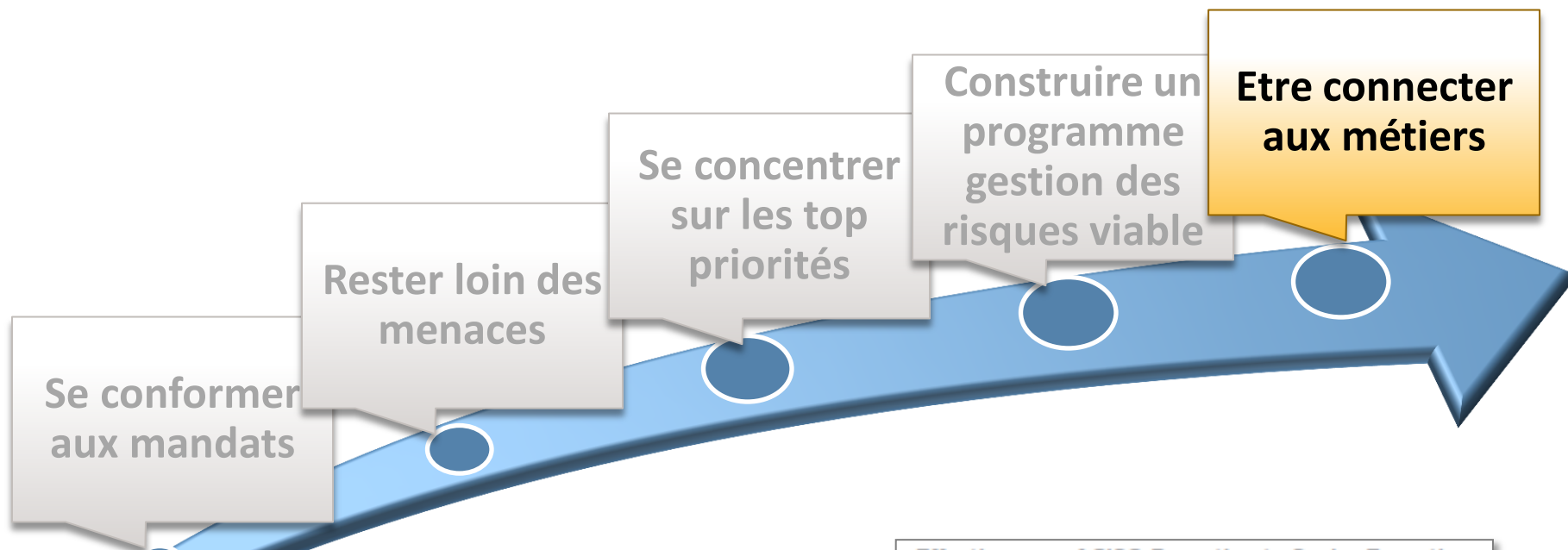
Se concentrer  
sur les top  
priorités

**Construire un  
programme  
gestion des  
risques viable**

Etre connecter  
aux métiers



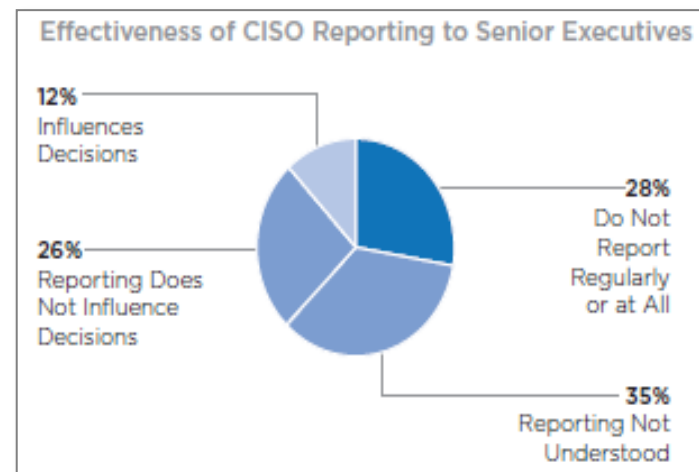
# De la conformité à la gestion du risque métier



**Difficulté à traduire les problèmes IT en termes métier**

**Seulement 1/8 des RSSI peuvent influencer les décisions métier**

*Source: Information Risk Executive Council, 2011*



# Les challenges qui limitent l'évolution

## Fonction en Silo

- Info Sec vu comme “Dr Non”
- Visibilité limitée dans l'exploitation
- Impossibilité de communiquer en termes métier

## Evaluations subjectives

- Enclin à erreur ou contestation
- Limitation de la vision instantanée unique
- Manque de métrique des responsabilités

## Collection manuelle des données

- Approche manuelle moins précise
- Vue incomplète
- Impossibilité de maintenir un environnement changeant



# Approche sur la gestion du risque et de la conformité

Parties prenantes



Audit



IT Ops/Sec Ops



Business

## PLANIFICATION

- Définir les objectifs métier et de risque
- Créer les politiques pour des mandats multiples
- Associer les contrôles

## RAPPORT

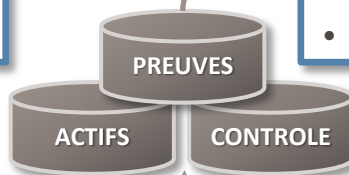
- Démontrer la conformité à plusieurs niveaux
- Corréler les risques à travers d'actifs métier
- Dashboards et rapports

## EVALUATION

- Identifier les déviations des standards techniques
- Identifier les vulnérabilités critiques
- Evaluer les contrôles procéduraux
- Combiner les données tierces

## REMEDIATION

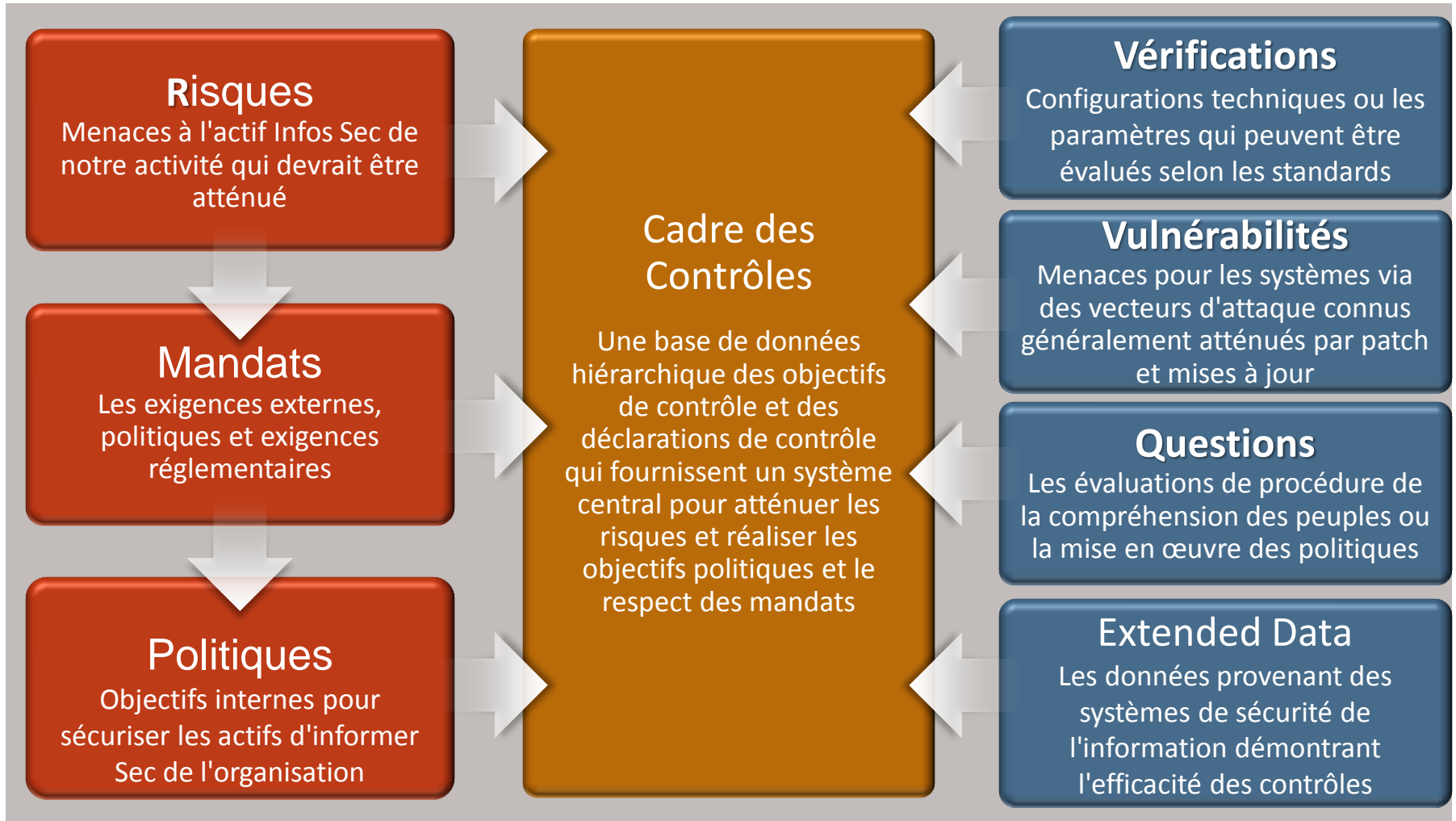
- Gestion de priorité basée sur le risque
- Suivi précis des insuffisances
- Intégration avec des outils de gestion de tickets d'incidents



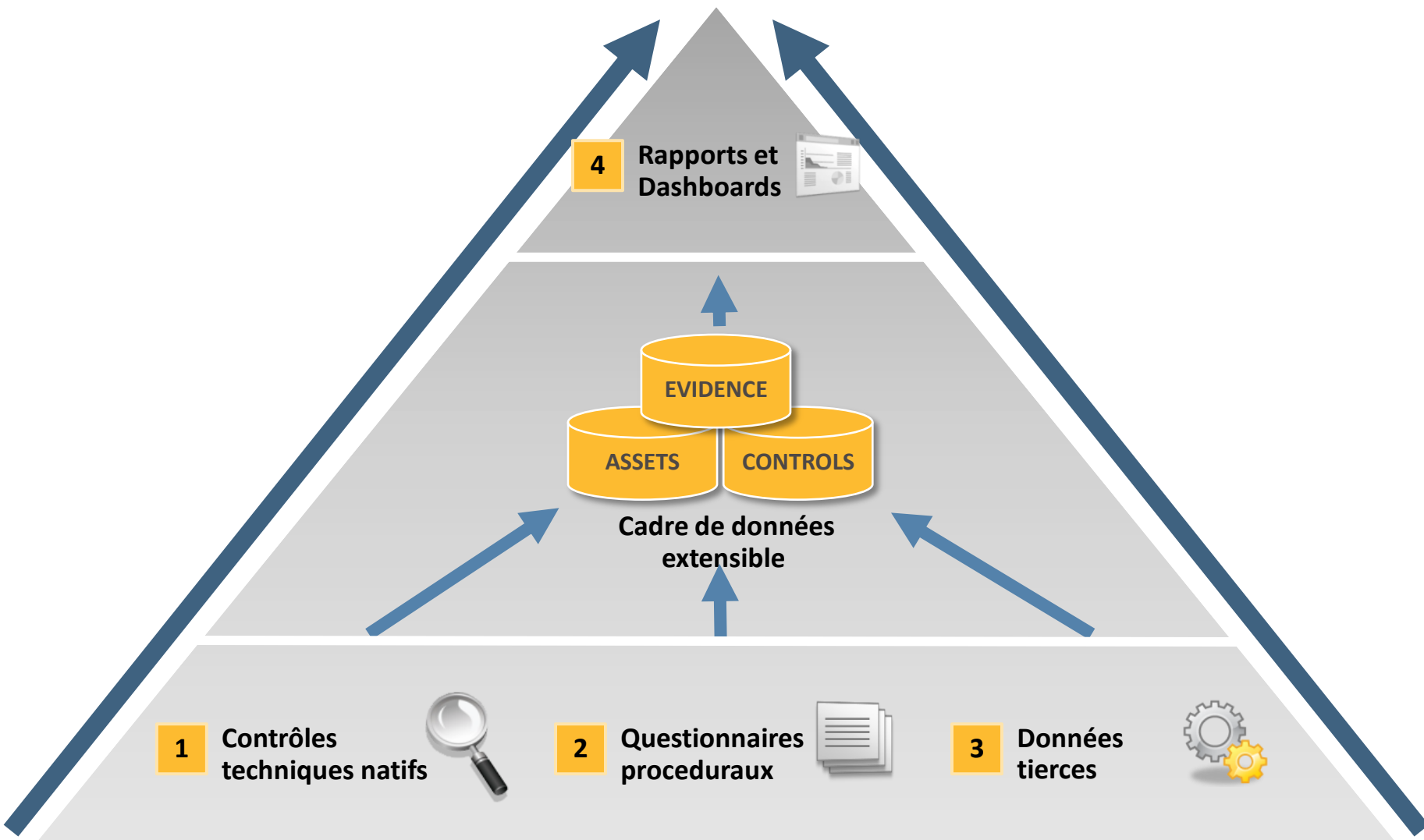
Environnement



# Le mécanisme IT GRC



# Approche bas vers le haut





# Gestion des risques – Cas client



## Prise de conscience des métiers

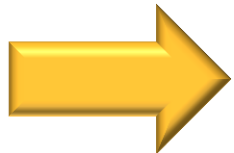
- Depuis cinq ans, Alain LA BU est directeur de la division Banque en Ligne qui représente 40 % du CA réalisé par la Banque.
- Lors d'un dîner, un ami lui parle d'un article de journal mentionnant la fuite de données dont a été victime une autre banque.
- Du coup, Alain se demande : « Est-ce que ça pourrait nous arriver ? »



# Gouvernance de l'entreprise

Le conseil d'administration voudrait s'assurer qu'aucun incident ne puisse avoir un effet négatif sur la confiance des clients et donc sur le cours de l'action.

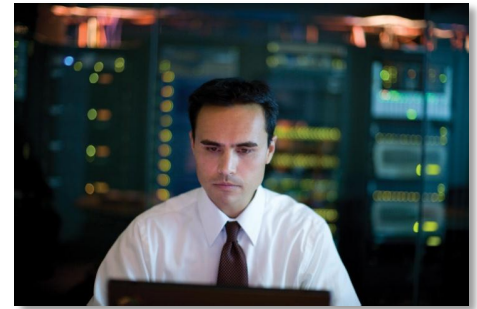
Lors de la prochaine réunion du conseil, Jean LE PATRON a donc mis à l'ordre du jour la question de la situation actuelle de sécurité de la banque.



Il demande donc à Paul LE CISO, le RSSI de la Banque, une **analyse détaillée des risques actuels**.

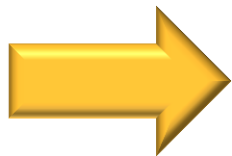
# Le CISO, chef d'orchestre

Paul LE CISO a peur que répondre à la demande du conseil d'administration lui prenne des mois, n'ayant à sa disposition que des moyens manuels pour évaluer les risques.



Il doit :

- Résumer les données des différents systèmes dans Excel
- Collecter les informations auprès des différents gestionnaires des domaines de sécurité (DSI, Services Généraux ...)
- Rationaliser les informations de risque sans affecter la précision
- Présenter les résultats en relation avec les processus métier de la banque et non dans le contexte IT

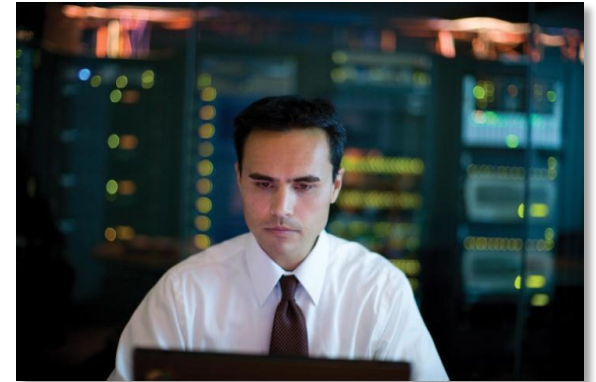


Comment **industrialiser** cette gestion complexe et aujourd'hui manuelle ?

# Les besoins de Paul LE CISO

L'industrialisation doit pouvoir :

- Définir les objectifs de risque afin de les gérer
- Comprendre et hiérarchiser les risques
- Définir une stratégie axée sur les risques pour éliminer les déviations



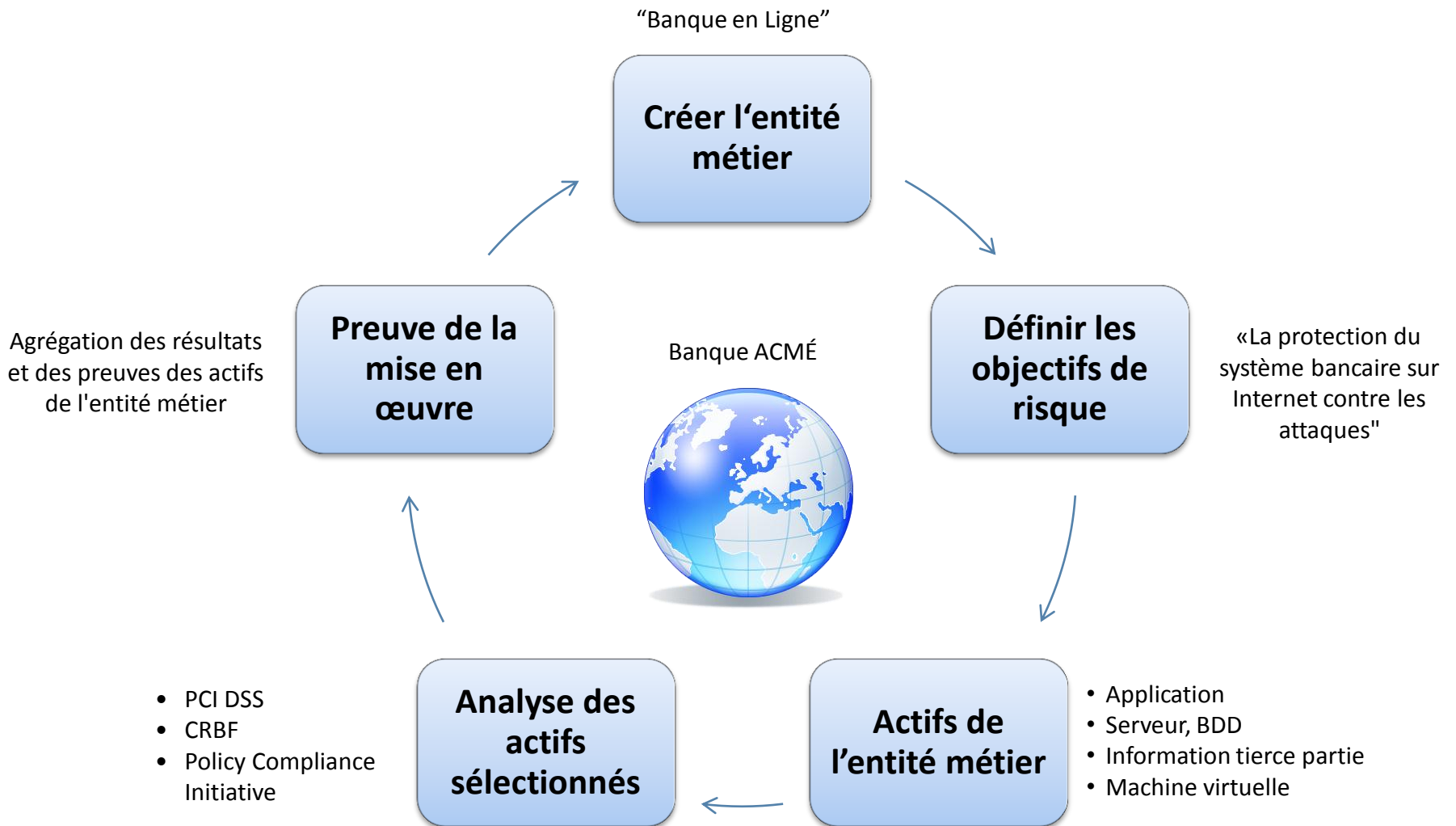
Alain LA BU vient lui poser la question de la protection du site de banque en ligne

Paul LE CISO décide donc de choisir **la banque en ligne comme pilote**



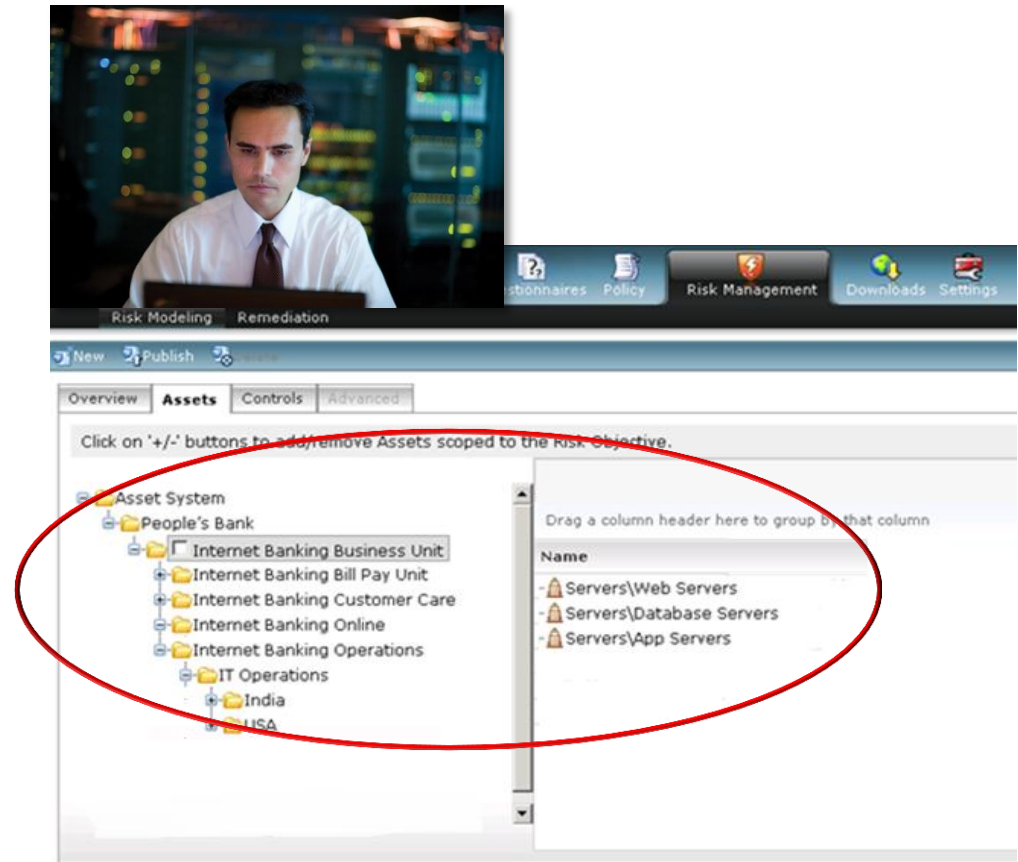
# Définir les objectifs et gérer les risques

# Processus de gestion du risque

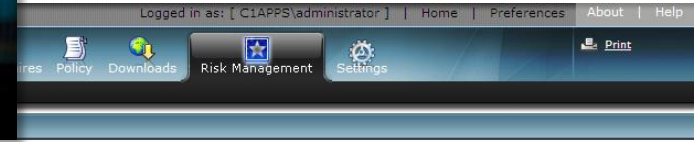
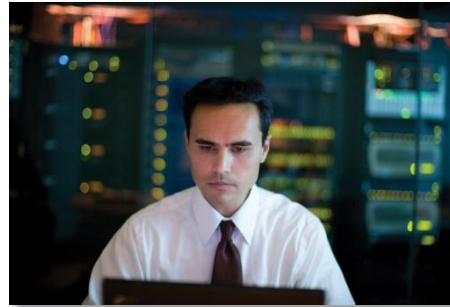


# Étape 1: création de l'entité métier

- Il génère d'abord une entité pour la division Banque en Ligne.
- Ainsi, il peut modéliser le risque de l'entité sur la base de groupes dynamiques d'actifs.



# Étape 2 : définition des objectifs de risque pour l'entité



-Protection des données clients

- Assurer la continuité de service 24/24

-Se prémunir de la fraude en ligne

-...

Risk objective	Owner	Target Date	Target Risk	Status
<input type="checkbox"/> Prevent Loss of Confidential customer data/Protect PII and sensitive...	Ashish Sharma	03/31/2012	04/25/2011	Saved
<input type="checkbox"/> Prevent financial frauds due to Non repudiation of transactions by cus...	Ashish Sharma	03/31/2013	05/06/2011	Saved
<input type="checkbox"/> Secure Business Continuity	Ashish Sharma	03/31/2014	05/15/2011	Published
<input type="checkbox"/> Prevent internal fraud resulting in financial and reputational loss	Chris Smith	03/31/2015	05/15/2011	Published
<input type="checkbox"/> Prevent Web based attacks to internet banking application	Chris Smith	03/31/2016	05/15/2011	Published

Account for and protect all IT assets

Overview Assets Control Objective Advanced

**Risk objective:** Prevent Loss of Confidential customer data/Protect PII and sensitive data

**Description:** Protect the integrity and confidentiality of personally identifiable information and sensitive information. All of the regulations that deal with privacy of PII data have an objective that such data is not disclosed to parties without the owners consent.

**Creation date:** 04/29/2011

**Requested by:** John Doe

**Created by:** Ashish Sharma

**Stake holders:** Ashish Sharma, Saneey Singh, Chris Smith

**Target date:** [Calendar icon]

**Threshold:** Low 3.2 Med 5.5 High

**Target Risk:** 5.0

**Impact:** Medium

**Likelihood:** Medium

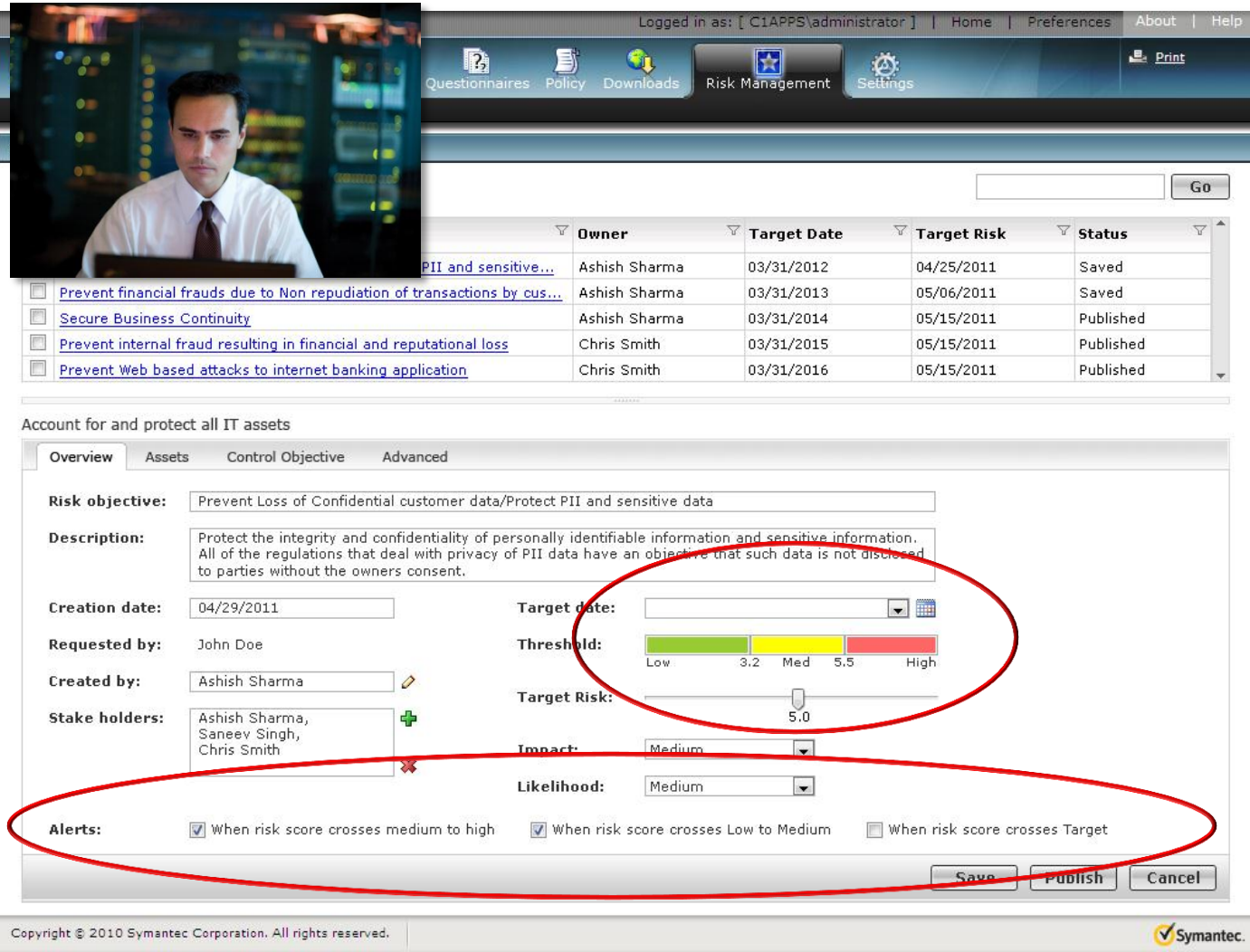
**Alerts:**  When risk score crosses medium to high  When risk score crosses Low to Medium  When risk score crosses Target

Save Publish Cancel

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec

# Étape 3 : définition des seuils et alarmes pour chaque objectif



The screenshot displays the Symantec Risk Management interface. At the top, a navigation bar includes 'Questionnaires', 'Policy', 'Downloads', 'Risk Management', and 'Settings'. A table lists several risk objectives with columns for Owner, Target Date, Target Risk, and Status. Below the table, the 'Control Objective' configuration view is shown for the objective 'Prevent Loss of Confidential customer data/Protect PII and sensitive data'. This view includes fields for Description, Creation date, Requested by, Created by, Stake holders, Target date, Threshold (a color-coded scale from Low to High), Target Risk (set to 5.0), Impact (set to Medium), and Likelihood (set to Medium). The Alerts section at the bottom has three checkboxes: 'When risk score crosses medium to high' (checked), 'When risk score crosses Low to Medium' (checked), and 'When risk score crosses Target' (unchecked). Red circles highlight the Threshold and Alerts sections. The footer contains the copyright notice 'Copyright © 2010 Symantec Corporation. All rights reserved.' and the Symantec logo.

	Owner	Target Date	Target Risk	Status
<input type="checkbox"/> PII and sensitive...	Ashish Sharma	03/31/2012	04/25/2011	Saved
<input type="checkbox"/> Prevent financial frauds due to Non repudiation of transactions by cus...	Ashish Sharma	03/31/2013	05/06/2011	Saved
<input type="checkbox"/> Secure Business Continuity	Ashish Sharma	03/31/2014	05/15/2011	Published
<input type="checkbox"/> Prevent internal fraud resulting in financial and reputational loss	Chris Smith	03/31/2015	05/15/2011	Published
<input type="checkbox"/> Prevent Web based attacks to internet banking application	Chris Smith	03/31/2016	05/15/2011	Published

**Risk objective:** Prevent Loss of Confidential customer data/Protect PII and sensitive data

**Description:** Protect the integrity and confidentiality of personally identifiable information and sensitive information. All of the regulations that deal with privacy of PII data have an objective that such data is not disclosed to parties without the owners consent.

**Creation date:** 04/29/2011

**Requested by:** John Doe

**Created by:** Ashish Sharma

**Stake holders:** Ashish Sharma, Saneev Singh, Chris Smith

**Target date:** [Calendar icon]

**Threshold:** Low 3.2 Med 5.5 High

**Target Risk:** 5.0

**Impact:** Medium

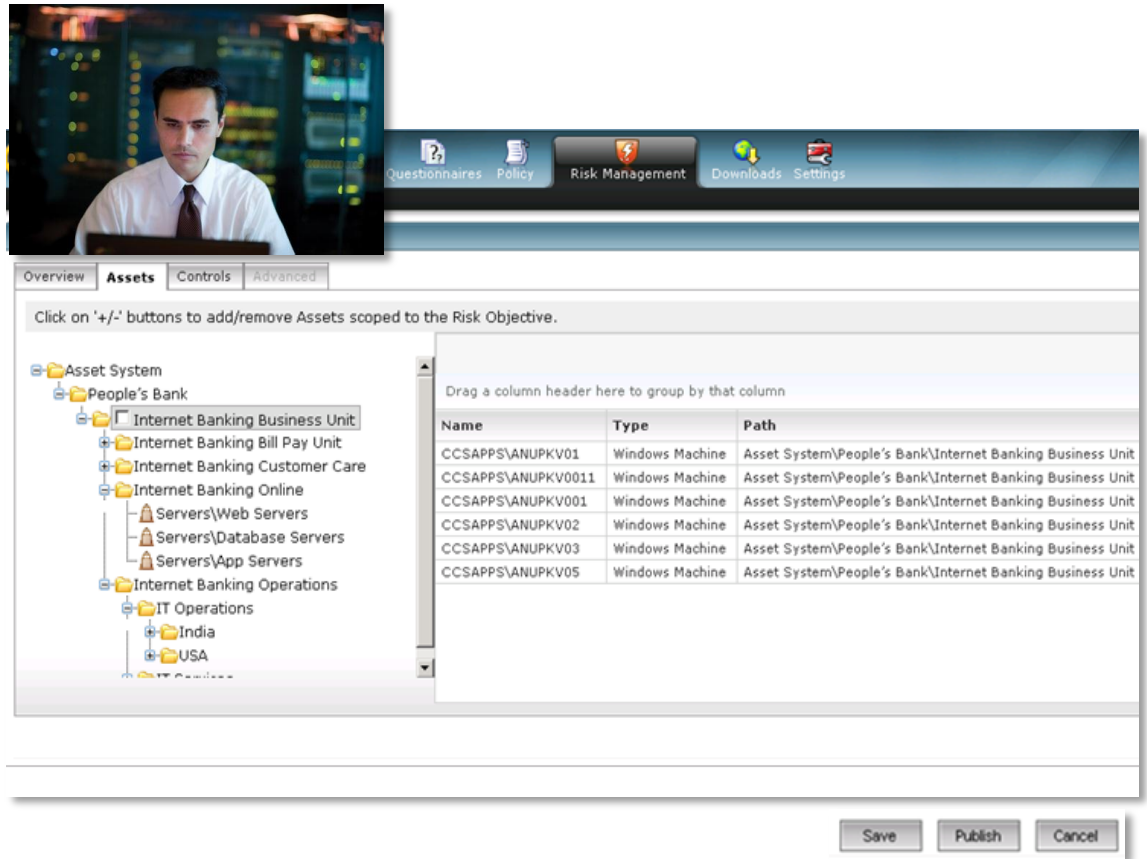
**Likelihood:** Medium

**Alerts:**  When risk score crosses medium to high  When risk score crosses Low to Medium  When risk score crosses Target

Buttons: Save, Publish, Cancel

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec.

# Étape 4 : création d'une hiérarchie des actifs



Les actifs peuvent être :

- des applications
- des bases de données
- des data Center
- des serveurs
- des machines virtuelles
- Etc...

Il prend notamment en compte les informations liées aux cartes de crédit des bases de données parce qu'il gère aussi la **certification PCI DSS**

# Étape 5 : sélection des contrôles

- Choissant seulement ceux qui sont liés à chaque objectif de risque.
- Si nécessaire, définir une **pondération relative** de chaque contrôle, ou même des **contrôles de compensation** appropriés.



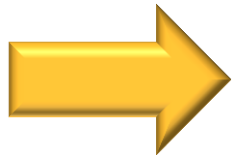
# Comprendre les risques et les hiérarchiser.



# L'intégration des données métiers

Paul LE CISO rencontre Alain LA BU pour :

- lui donner un aperçu de **l'état actuel** des risques et menaces,
- valider ensemble le **risque acceptable** pour chaque actif
- définir un plan de **priorité de remédiation** en fonction des risques mesurés

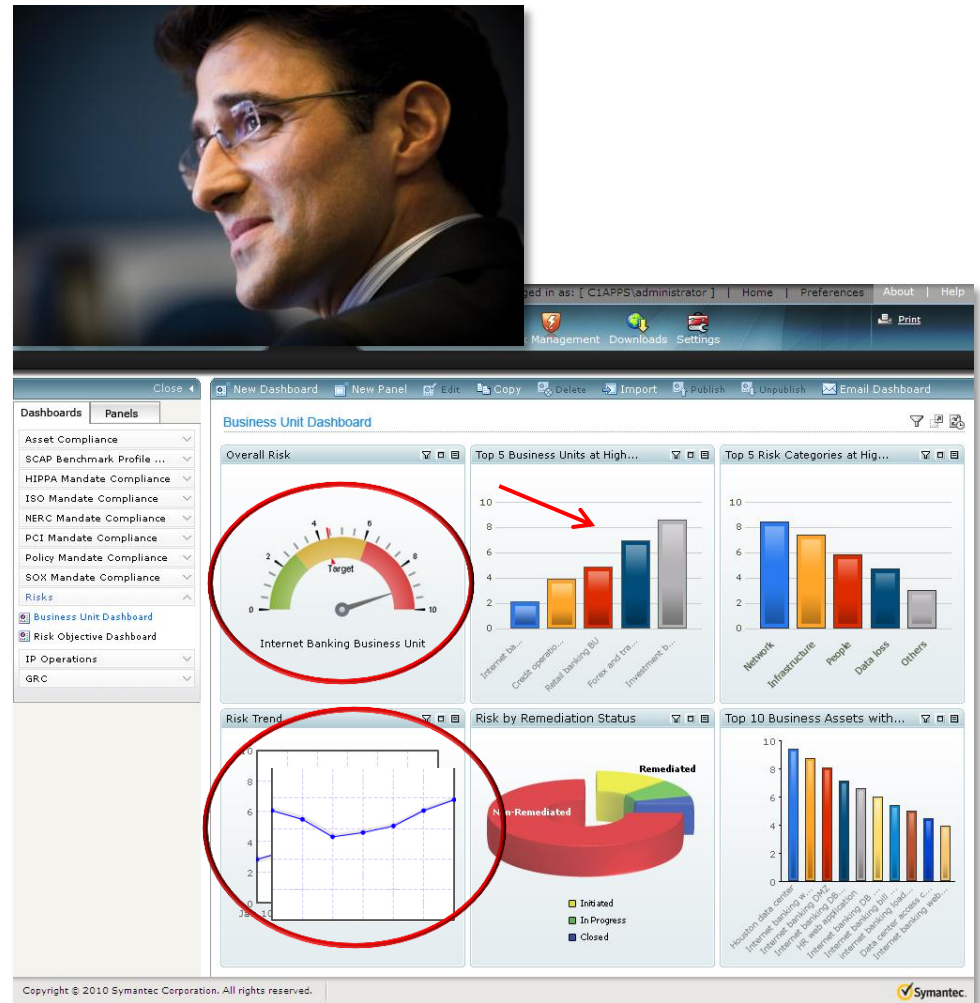


Le système est opérationnel et les premiers résultats commencent à être disponibles

# Piloter sa stratégie de gestion de risque

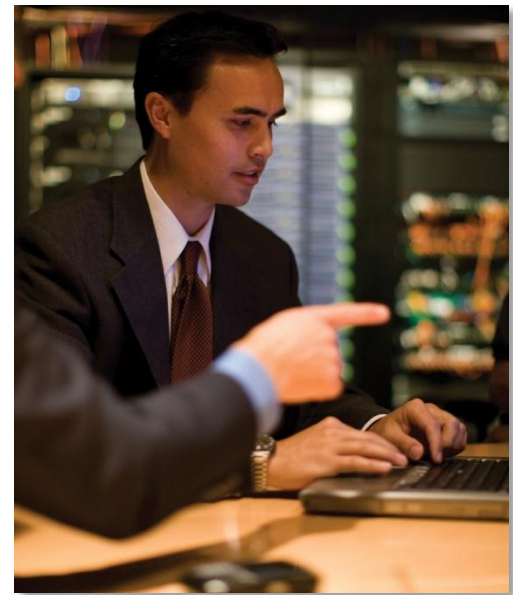
# Tableau de bord

- Le tableau de bord affiche en permanence les valeurs de risque agrégées pour Alain LA BU
- Le seuil de risque a été fixé à **4,5** mais il est actuellement à **9**
- Dans le même temps, son métier a le plus haut niveau de menace de la banque.
- Un regard rapide sur la tendance montre une augmentation du risque.



# Prise de conscience des métiers et remédiation

- Alain LA BU a maintenant une vision claire des risques de sa division, la banque en ligne.
- Face au risque élevé, il doit donc allouer le budget nécessaire à Paul LE CISO pour mettre en place le plan d'action adéquat.



# Par où commencer ?

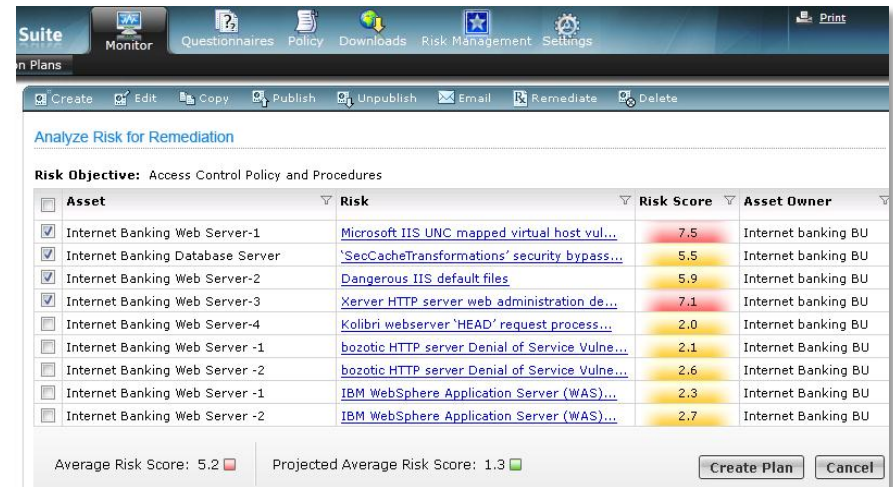
- Le tableau de bord montre les actifs de l'entreprise ayant le risque actuel le plus élevé
- M. LE CISO et M. LA BU peuvent donc analyser les causes avec plus de précision



# Au niveau IT, d'où viennent ces risques ?

• Lors de l'analyse de l'information de risque des actifs frontaux internet, on distingue :

- 4 machines avec un **risque modéré**
- 2 dont le **seuil d'alarme a été dépassé**



The screenshot shows the 'Analyze Risk for Remediation' window in Symantec Suite. The table below lists the assets, their associated risks, risk scores, and asset owners. The risk scores are color-coded: red for scores above 5.0 and yellow for scores below 5.0.

Asset	Risk	Risk Score	Asset Owner
<input checked="" type="checkbox"/> Internet Banking Web Server-1	Microsoft IIS UNC mapped virtual host vul...	7.5	Internet banking BU
<input checked="" type="checkbox"/> Internet Banking Database Server	'SecCacheTransformations' security bypass...	5.5	Internet banking BU
<input checked="" type="checkbox"/> Internet Banking Web Server-2	Dangerous IIS default files	5.9	Internet banking BU
<input checked="" type="checkbox"/> Internet Banking Web Server-3	Xerver HTTP server web administration de...	7.1	Internet banking BU
<input type="checkbox"/> Internet Banking Web Server-4	Kolibri webservers 'HEAD' request process...	2.0	Internet banking BU
<input type="checkbox"/> Internet Banking Web Server -1	bozotic HTTP server Denial of Service Vulne...	2.1	Internet Banking BU
<input type="checkbox"/> Internet Banking Web Server -2	bozotic HTTP server Denial of Service Vulne...	2.6	Internet Banking BU
<input type="checkbox"/> Internet Banking Web Server -1	IBM WebSphere Application Server (WAS)...	2.3	Internet Banking BU
<input type="checkbox"/> Internet Banking Web Server -2	IBM WebSphere Application Server (WAS)...	2.7	Internet Banking BU

Average Risk Score: 5.2 ■    Projected Average Risk Score: 1.3 ■    Create Plan Cancel

Il est donc évident de **remédier prioritairement** les menaces impactant ces 2 actifs.

# Projection de réduction de risque

- Alain LA BU veut voir son entité revenir vite à un **niveau de risque acceptable**

- Paul LE CISO exécute une analyse « **what-if** » visant à déterminer l'impact de la correction du risque le plus élevé

=> réduction du score de risque de **5,2** à **1,3**

The screenshot shows the Symantec Control Compliance Suite Risk Management interface. At the top, there is a navigation bar with icons for Dashboards, Questionnaires, Policy, Risk Management, Downloads, and Settings. Below this, the 'Remediation' tab is active. The main content area displays a table titled 'Remediation Plans' with columns for Plan Name, Assigned to, and Risk Score (Current and Projected). The table lists five remediation plans, each with a checkbox, a description, an assigned person, and two risk scores. A red circle highlights the 'Projected residual risk' value of 1.3 at the bottom of the interface.

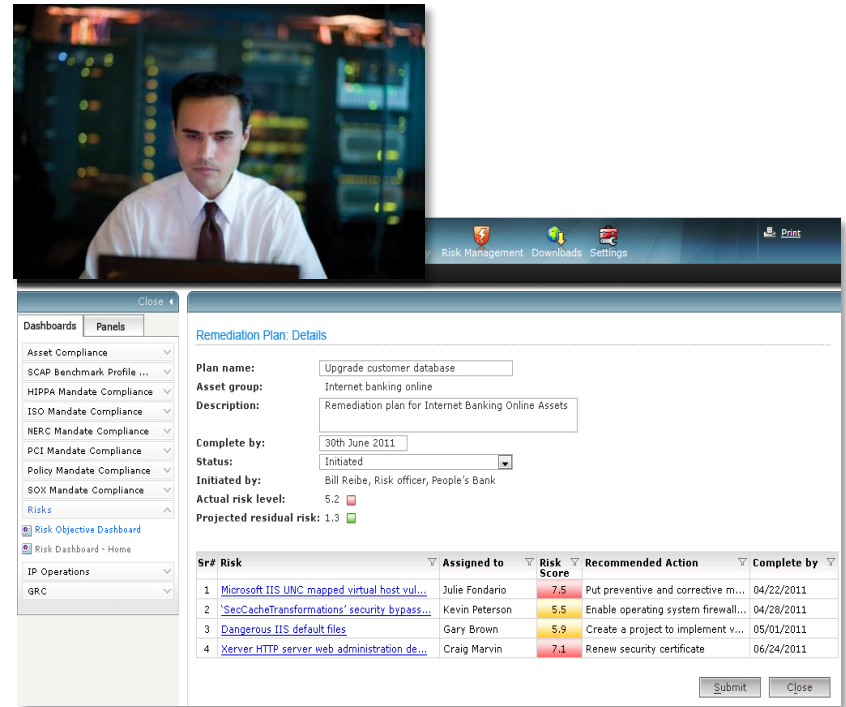
Plan Name	Assigned to	Risk Score	
		Current	Projected
<input type="checkbox"/> <a href="#">Remove XSS vulnerabilities from Email Server</a>	Jim Arnold	7.5	1.5
<input type="checkbox"/> <a href="#">Apply latest patch to internet banking web server</a>	Peggy Kirk	5.5	1.0
<input checked="" type="checkbox"/> <a href="#">Upgrade customers database 1 to SP2</a>	Roland Brown	5.9	1.1
<input type="checkbox"/> <a href="#">Apply certificates to all webserver for online store</a>	Michael Smith	7.1	1.2
<input type="checkbox"/> <a href="#">Apply latest patch on external firewall</a>	Jack Russel	5.1	2.8

Actual risk level: 5.2 ■    Projected residual risk: 1.3 ■

Ainsi, l'entité de M. LA BU serait de retour dans une zone acceptable

# Plan de remédiation

- Étant donné qu'ils ont convenu d'une stratégie pour résoudre les divergences, Paul LE CISO les détaille et identifie les responsables pour les changements.



The screenshot displays a web-based risk management application. At the top, there is a navigation bar with icons for Risk Management, Downloads, Settings, and a Print button. Below this, the main content area is titled 'Remediation Plan: Details'. It contains several fields: Plan name (Upgrade customer database), Asset group (Internet banking online), Description (Remediation plan for Internet Banking Online Assets), Complete by (30th June 2011), Status (Initiated), Initiated by (Bill Reibe, Risk officer, People's Bank), Actual risk level (5.2), and Projected residual risk (1.3). A table below lists four risks with their assigned owners, risk scores, recommended actions, and completion dates.

Sr#	Risk	Assigned to	Risk Score	Recommended Action	Complete by
1	Microsoft IIS UNC mapped virtual host vul...	Julie Fondario	7.5	Put preventive and corrective m...	04/22/2011
2	"SecCacheTransformations" security bypass...	Kevin Peterson	5.5	Enable operating system firewall...	04/28/2011
3	Dangerous IIS default files	Gary Brown	5.9	Create a project to implement v...	05/01/2011
4	Xerver HTTP server web administration de...	Craig Marvin	7.1	Renew security certificate	06/24/2011



# Visualisation permanente de la gestion des risques

- Paul LE CISO a créé une entité dans le tableau de bord pour Alain LA BU lui permettant de suivre les processus individuels de réduction des risques
- Ensemble, ils sont confiant de pouvoir donner un statut clair au conseil sur la menace actuelle avec un aperçu des réductions en cours
- Paul LE CISO créé également un tableau de bord pour le Directeur Général et les opérations informatiques afin qu'ils suivent également ces processus



# Une bonne gouvernance dans la gestion des risques IT

- Paul LE CISO a donné à M. LE PATRON les informations détaillées dont il avait besoin pour son rapport au Conseil
- Parce que le suivi des risques est maintenant automatisé, M. LE PATRON peut aussi promettre d'informer plus fréquemment le conseil sur la position de menace actuelle
- Le conseil a donc toute confiance que tout a été mis en œuvre pour prévenir les risques



# Relever les défis

1

## Meilleure Visibilité

- **Convertir l'impact des risques IT dans des termes métier**
- Conduire la connaissance, l'action et la responsabilité par des métriques ciblés
- Eliminer les silos entre la sécurité et l'opérationnel

2

## Automatisation

- **Automatiser la collection et le cycle de vie de la remédiation**
- Faciliter la collection continue pour une meilleure fiabilité
- Répondre rapidement aux question liés aux problèmes

3

## Prioritisation des risques

- **Tirer des conclusions conduites par des données défendables**
- Prioriser les problèmes en se basant sur des risques métiers plus que techniques
- Remédier les risques identifiés prioritaires



# Q&A

## Merci de votre attention!

**Copyright © 2012 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.