

# L'amélioration continue de la sécurisation du système d'information



## Conseil et audit Sécurité

Les listes sans fin de risques auxquels sont exposés les Systèmes d'Information sont légion et facilement accessibles sur le Web. Certaines sociétés vont jusqu'à les mettre au cœur de leur communication. Cependant, l'identification des risques n'est que l'une des facettes d'une politique de Sécurité bien pensée. Il faut les pondérer à l'aune de leurs impacts sur les activités de l'organisation et des coûts à engager pour les réduire.

### Enjeux, risques et coûts

Une organisation qui réfléchit à la sécurisation de son Système d'Information doit le faire sous la triple contrainte des coûts, des menaces et des caractéristiques de son S.I. en termes d'enjeux et de vulnérabilités. Les démarches uniquement techniques ou organisationnelles ne permettent pas de couvrir toutes les failles, même si ces dernières ont été identifiées. Obtenir une solution qui fasse le bon arbitrage entre les coûts, les risques et les impacts relève donc d'une démarche globale faisant intervenir de multiples acteurs de l'organisation et intégrant les évolutions continues de l'entreprise.

### Le Système de Management de la Sécurité de l'Information

Sécuriser un S.I. doit s'inscrire dans une démarche d'amélioration continue de type Plan-Do-Check-Act (PDCA), démarche supportée pleinement par les normes ISO27001 et ISO27002. Le système comprend trois axes répondant aux contraintes de l'entreprise :

- éléments communs à tout système de management : procédures, documentation, indicateurs, programme d'audit, engagement de la Direction, mobilisation des ressources, revues, etc. ;

- définition de la politique sécurité : analyse de risque, décisions sur les plans d'actions de réduction des risques, validation des risques résiduels ;
- plans d'actions de sécurisation : solutions techniques (antivirus, pare-feu, etc.), procédures organisationnelles (workflow d'approbation, règle d'utilisation, etc.).

### Bull Réseau et Sécurité : une approche complète du système de management de la sécurité

Les consultants et experts de Bull Réseau et Sécurité aident les organisations à définir, mettre en œuvre et améliorer la sécurisation de leur S.I. et à mettre en place des systèmes de management de la sécurité adaptés à chaque contexte.

Au cœur de leur savoir-faire :

- la maîtrise des méthodologies du marché, fruits des meilleures pratiques européennes, comme MEHARI™ du CLUSIF et EBIOS® de la DCSSI ;
- l'expertise des technologies de la sécurité et des réseaux : pare-feu, VPN, gestion des accès et des identités, ToIP, VoIP, plan de continuité et de reprise ;
- l'expérience des missions de conseil et d'audit et la capacité à gérer des projets complexes et structurants.

BULL RESEAU ET SECURITE



Architect of an Open World™

1

## Le conseil stratégique

Les consultants de Bull interviennent dans des missions de conseil stratégiques auprès des Directions Générales ou Métier pour positionner la stratégie SSI de l'entreprise, ou auprès des Directions des Systèmes d'Information afin de piloter et mettre en œuvre les recommandations, en lien avec les processus métier. Les experts certifiés de Bull aident ainsi les organisations à :

- définir et mettre en place la politique de sécurité ;
- définir le plan stratégique et le schéma directeur de sécurité ;
- définir et mettre en place la charte utilisateur ;
- effectuer les analyses de risque ;
- définir et mettre en place le plan de sensibilisation des utilisateurs ;
- définir et mettre en place le Système de Management de la sécurité ;
- effectuer des études spécifiques (ROI, analyse de processus, etc.).

2

## Les audits techniques

Les consultants de Bull analysent l'impact des technologies sur la sécurité des S.I. et déterminent le niveau de confidentialité, d'intégrité et de disponibilité des solutions.

- L'audit d'architecture permet d'obtenir un diagnostic de la sécurité d'une plate-forme ou d'une solution : points faibles et forts des maillons de la chaîne applicative, recensement et qualification des vulnérabilités, identification des parades techniques.
- Le test de vulnérabilité permet d'identifier les failles présentes (serveur, routeur, etc.). Il est effectué en interne ou en externe et est réalisé sur une ou plusieurs cibles.
- Le test d'intrusion qualifie le niveau de sécurité du S.I depuis l'extérieur ou l'intérieur de l'entreprise. Il s'appuie sur une méthodologie rigoureuse permettant d'assurer le non-débordement, la traçabilité des actions menées, le bon niveau des livrables, etc.
- L'audit de code assure une relecture du code source de l'application sous l'angle de la sécurité et identifie les techniques de programmation n'assurant pas une sécurité suffisante. Il permet de contrôler la présence de vulnérabilités susceptibles d'entraîner des problèmes de sécurité, de vérifier l'absence de « porte dérobée », intentionnelle ou non.

# 6 pôles d'excellence globale de système

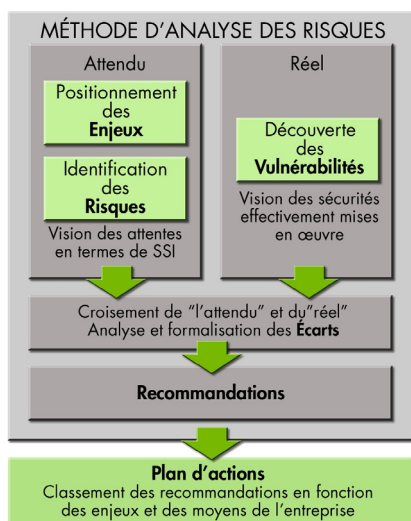
3

## Le Conseil et l'audit réseau

Bull accompagne les organisations dans la réalisation de toutes les prestations réseaux, qu'elles soient fonctionnelles ou techniques.

Les compétences des intervenants sont maintenues à jour grâce aux programmes de certification des constructeurs télécom et aux formations méthodologiques définies par les organismes de standardisation.

- Le conseil en réseaux a pour objectif de structurer les besoins et de cerner les objectifs propres à chaque organisation. Les consultants réalisent des schémas directeurs et des cahiers des charges, produisent les spécifications fonctionnelles et techniques, animent les projets dans leur globalité. Ils savent bâtir des solutions à l'état de l'art et mutualiser l'ensemble des services sur un même réseau IP.
- L'audit technique de réseaux permet de réaliser des analyses de performances, de suivre le respect des engagements (SLA), de recenser la typologie des flux applicatifs, de produire des rapports de métrologie et matrices de trafic, de réaliser des opérations de 'troubleshooting'.



Démarche générique d'une méthode d'analyse de risques (source Bull)

# pour une approche sécurisation du d'information

4

## Le plan de continuité d'activité

Bull aide à maîtriser l'ensemble des étapes de sa mise en œuvre.

- L'étude de cadrage permet de préciser les périmètres métier, géographiques et applicatifs du projet, d'analyser les risques et les attentes puis de définir l'organisation.
- Le lancement détermine l'organisation du projet, sa planification et ses enjeux.
- L'analyse des risques et le bilan d'impact sur l'activité permettent de classer les applications selon leur criticité et d'en déduire les orientations.
- La mise en œuvre des solutions techniques et organisationnelles, après analyse des risques. Il faut ensuite formaliser le PCA ou le PRA, formaliser le plan de test et valider le plan de continuité.
- Le Maintien en Condition Opérationnel, inclut la documentation, l'administration et le suivi du plan de continuité d'activité, ainsi que la réalisation du programme de tests.

5

## La ToIP/VoIP

C'est aujourd'hui une réalité incontournable, en raison du nécessaire renouvellement des PABX. Les experts de Bull interviennent en tant qu'assistants à la maîtrise d'ouvrage sur les différentes étapes du projet.

- L'analyse de l'existant et des besoins permet de recenser les architectures techniques et applicatives, d'appréhender les besoins nouveaux, les contraintes ainsi que les attentes des utilisateurs dans la pratique quotidienne de leurs métiers.
- L'élaboration de la stratégie et du dossier de consultation. Bull met à profit son expérience pour définir avec l'entreprise la stratégie de l'appel d'offre : type de marché et de procédure, mode de publication, etc. Les pièces techniques et administratives relatives à la consultation peuvent alors être rédigées.
- L'assistance à la consultation. Quel que soit le mode de consultation, Bull élabore et rédige les grilles techniques d'évaluation pondérées qui permettront l'appréciation objectives des offres.
- L'assistance au déploiement consiste à assurer une interface unique avec la Maîtrise d'ouvrage pour la gestion du projet et à apporter une assistance et une expertise technique telles que approbations et acceptations des actions et documentations.

6

## Le conseil en IAM

L'enjeu est de maîtriser l'accès aux données via les applications de l'organisation. Les consultants de Bull assistent les organisations dans la définition de leurs besoins, l'élaboration de leur stratégie et le déploiement des solutions choisies.

- L'analyse de l'existant et des besoins détermine les besoins en fonction des contraintes réglementaires, des objectifs de l'organisation et de l'infrastructure existante. Un scénario global de l'infrastructure peut alors être construit.
- L'élaboration de la stratégie et des cahiers des charges, en fonction du scénario choisi et pour un ou pour plusieurs domaines de la Gestion des Identités et des Accès : annuaire d'entreprise, authentification forte, contrôle d'accès et SSO, provisionnement et Rôles, privilèges RBAC, etc.

Bull assiste l'entreprise dans les phases les plus critiques de chaque projet :

- schéma de l'annuaire et règles de mises à jour ;
- validation de la chaîne d'authentification forte ;
- intégration des applications dans le moteur de SSO ;
- définition des processus de gestion des utilisateurs ;
- création de la politique RBAC (rôle & privilèges).

# Bull Réseau et Sécurité, l'acteur de la sécurisation de votre système d'Information

## **Accompagne**

les organisations dans la mise en œuvre de leur projet de sécurisation et de mise en place de Système de Management de la Sécurité.

## **Utilise**

les méthodes et normes du marché (MEHARI™, EBIOS®, ISO2700x, etc.) pour mettre en place les rouages de l'amélioration continue.

## **S'appuie**

sur une équipe de consultants réseau et sécurité, formés et certifiés aux principales méthodes et technologies du marché.

## **Conseille**

les Directions Générales, Directions métier et Directions des Systèmes d'Information dans la définition de plans de sécurisation pertinents et totalement adaptés à chaque problématique.

## **Mène**

les audits, les études et les analyses préalables à toutes décisions.

## **Gère**

les projets complexes et stratégiques.

## **Maintient**

les plans de continuité de service en condition opérationnelle.

## **Sensibilise**

l'ensemble des acteurs de l'entreprise aux nouvelles pratiques et les forme aux technologies de la sécurité.

Contact : Pôle Conseil et  
Audit en Réseau et Sécurité  
Bull-Conseil-Audit@bull.net  
33 (0)130 80 32 96