1. **Contexte**

ACM vient de recevoir un bon de commande pour effectuer une série d’audit et test d’intrusion pour une entreprise multisites avec 4 sites à l’intérieur du pays et le site central à Conakry.

1. Audit organisationnel et physique ;
2. Une analyse des risques Cyber ;
3. Un audit des fournisseurs ;
4. Un audit a blanc ISO 27001 ;
5. Tests d’intrusion externes pour chaque site.
6. **AFRICAN CYBERSECURITY MARKET**

L’ACM est une entreprise spécialisée en Cybersécurité, née du désir de mettre à disposition du marché africain des offres spécifiques et innovantes en matière de sécurité des systèmes d’information, ceci en s’appuyant sur l’expertise de son équipe dynamique composée de spécialiste et certifiés en Cybersécurité.

Les services fournis par l’ACM sont :

* Cyber Stratégie
* Cyberdéfense
* Cyber Offensive
* Cyber Opérationnel
* Sensibilisation
* Cyber Training

1. **Mission**

Il s’agit de faire :

* un audit organisationnel ;
* une analyse des risques (Bilan de santé cybersécurité) ;
* un audit des fournisseurs ;
* un audit à blanc ISO 27001 ;
* Test d’intrusion (Pentest).

1. **Les parties prenantes :**

* African Cybersecurity Market
* Entreprise
* Fournisseurs

1. **Méthodologie de prestation**

Pour la mise en œuvre de ce projet, les différents acteurs et leur mode d’organisation doivent permettre une réalisation optimale.

Pour ce faire, le projet sera organisé comme suit :

* 1. **Une équipe projet**

Qui est l’instance porteuse du projet qui prend en charge le pilotage des activités, le contrôle de la conformité et la qualité des livrables convenus et la communication au-delà

* 1. **Périmètre du projet**

Le projet d’audit et de test d’intrusion consiste à faire l’état des lieux de l’ensemble des systèmes d’information.

1. **Outils utilisés pour la mission** :
2. **Référentiel ISO 27001**
3. **Système d’exploitation**

* Windows
* Linux
* Mac
* Virtual machine

1. **Logiciel**

* Nessus
* Nexpose
* Openvas
* Owasp
* Nikto
* Burpsuite
* Metasploit Framework

1. **Risque du projet**

Les risques font partie des [informations essentielles](https://www.planzone.fr/blog/quelles-informations-un-chef-de-projet-doit-avoir-sur-son-projet) à prendre en compte. Dès le démarrage du projet, nous devons dresser une liste plus exhaustive de tous les événements générateurs de risques.

Pour cela, il faut rassemblez toute l’équipe et lancez un brainstorming afin de répertorier tous les dangers possibles susceptibles de se produire.

On peut distinguer différents types de risques :

* Financiers : coût supérieur à l'estimation, manque de budget, etc.
* Humains : manque de compétences, absentéisme, démission au cours du projet, conflits au sein de l'équipe, etc.
* Temporels : retards des sous-traitants ou des fournisseurs, mauvaise estimation des délais, etc.
* Techniques : logiciel inadapté, pannes, matériel obsolète, etc.
* Juridiques : réglementations et lois à respecter, faillite d'un fournisseur, etc.
* Environnementaux : impacts négatifs du projet sur l'environnement, ou environnement ayant un impact sur le projet (inondation)
* Organisationnels : changement dans la politique de l'entreprise, changements économiques, etc.
* **Évaluer et hiérarchiser les risques**

Une fois votre liste de menaces potentielles établie, analysez chacune d'elle afin d'estimer leurs impacts sur les délais, les coûts et les spécifications techniques du projet. A ce stade, nous pourrons ainsi séparer les risques non fondés des risques réels et susceptibles d’affecter le déroulement du projet.

Ensuite, évaluer la probabilité d'apparition de chacun des risques répertoriés et leur gravité en matière d'impacts, de dommages et de conséquences sur les objectifs de la mission.

**Le but est de se concentrer sur les risques les plus importants et les plus probables, agir efficacement pour empêcher qu'ils ne se produisent et déterminer des actions à mener en priorité pour les maîtriser.**

* **Traiter les risques**

Le traitement des risques peut se faire de trois façons :

* **Éliminer le risque**: repousser la menace par la mise en œuvre d'actions visant à supprimer les causes du risque.
* **Limiter les effets du risque**: vous ne pouvez pas empêcher le risque de se produire, mais vous pouvez limiter son impact négatif sur le projet et le rendre plus supportable.
* **Réviser le projet :** pour éviter le risque, la seule option est de réorienter votre projet, de le simplifier ou de trouver des alternatives moins risquées.
* **Suivre et contrôler les risques**

Le suivi des risques doit se faire tout au long du projet. Au fur et à mesure que votre projet avance, les risques potentiels évoluent. Certains peuvent disparaître, d'autres apparaître, ceux considérés comme faibles peuvent devenir de réelles menaces et inversement.

Révisez régulièrement les risques en mettant à jour votre liste de menaces potentielles, en les réévaluant et en vous assurant que les actions de prévention sont toujours adaptées. Il est important d'assigner une ou plusieurs personnes sur cette mission afin d'être sûr qu'elle sera rigoureusement effectuée.

**Quatre (4) risques majeurs :**

* Vol ou destruction de données ;
* Indisponibilité ;
* Usurpation d’identité ;
* Fraude.

1. **Description des ressources**

Les ressources de ce projet peuvent être réparties en trois (3) catégories :

* Humaines
* Matériels
* Financières

Le Project Manager Cybersec a la responsabilité de correctement répartir ces ressources sur chaque tâche pour une rentabilité et une exécution dans les délais.

* **Les ressources humaines**

Il s’agit de l’ensemble des acteurs qui travaillent sur le projet.

Il est indispensable de s’entourer d’une équipe pluridisciplinaire qui possède les compétences, l’expérience et le savoir-faire indispensables à la réalisation du projet.

Notons également que la durée d’une tâche dépendra du nombre de ressources humaines qui lui est affecté. Par exemple, une personne seule mettra deux ans à construire une maison alors que dix personnes mettront seulement 3 mois.

* **Les ressources matérielles**

Les ressources matérielles englobent tout ce que possède déjà l’entreprise, mais également tout ce qui sera nécessaire à la réalisation du projet : lieux (salles, bâtiments, terrains, etc.), matériels et équipements (ordinateurs, téléphone, etc.), logiciels, outils, machines, etc.

Cela implique différents types d’investissements comme l’achat ou la location de matériels, d’outils.

Ces ressources matérielles seront déterminées en fonction des différentes tâches, mais aussi en fonction du budget alloué au projet, des délais et de la qualité souhaitée.

* **Les ressources financières**

Il s’agit du budget alloué ce qui englobe tous [les coûts](https://www.planzone.fr/blog/comment-estimer-cout-projet) et les dépenses engendrées par le projet :

* L’achat et la location de ressources matérielles
* Les éventuels frais de déplacement

1. **Démarche de la mission**

**Etape1** : Initialisation de la démarche

Consiste à définir clairement les objectifs et les enjeux avec l’ensemble des parties prenantes. Tous les éléments nécessaires au bon déroulement du projet.

Taches à exécuter :

* Rédiger le cahier des charges
* Identifier les besoins

Livrables : note de cadrage

**Etape 2 :** Analyse et diagnostic

Consiste à détecter les faiblesses du système d’information, en réalisant un état des lieux qui servira de point de point de départ à l’amélioration de l’infrastructure cliente

Tâches à exécuter :

Recueillir et analyser les différents les éléments documents relatifs à la description du système d’information, les normes utilisés, l’inventaire des ressources et des actifs, identifier les processus existants.

**Etape 3 :** Procéder à l’audit

Consiste à tester le système d’information pour identifier les problèmes de sécurité et de performance. Différents aspects du système d’information pourront être passés au crible :

* Audit organisationnel et physique ;
* Une analyse des risques Cyber ;
* Un audit des fournisseurs ;
* Un audit a blanc ISO 27001 ;
* Tests d’intrusion externes pour chaque site.

**Etape 4** : Rédiger le rapport

La concrétisation se matérialise à travers un rapport comprenant les différentes analyses et constats qui sont apparus l’audit :

1. **Planning**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PHASES | ACTIVITES | ECHEANCES | RESPONSABLE | RESSOURCES | OBSERVATIONS |
| Initialisation de la démarche | Rédiger le cahier des charges.  Identifier les besoins. | 1 semaines | TEAM ACM |  |  |
| Analyse et diagnostic | Recueillir et analyser les différents les éléments documents relatifs à la description du système d’information, les normes utilisés, l’inventaire des ressources et des actifs, identifier les processus existants. | 1 semaines | TEAM ACM |  |  |
| Procéder à l’audit | Faire le pentest | 1 semaines | TEAM ACM |  |  |
| Clôture | Rédiger le rapport d’audit et faire des recommandations | 1 semaines | TEAM ACM |  |  |