De l'Audit de sécurité à l'Evaluation des risques et la Politique de Sécurité des SI

Dr. (MC) Ing. S. Arnaud M. R. AHOUANDJINOU
Expert Cybersécurité et système intelligent
Chef Département Sécurité Informatique/ IFRI, UAC, Bénin
Directeur Adjoint du Laboratoire LRSIA/ IFRI, UAC, Bénin

ATELIER DE FORMATION DES DELEGUES A LA PROTECTION DES DONNEES PERSONNELLES (DPO), APDP, Cotonou (Bénin), 20-12-2022

Plan

- Introduction à la sécurité du SI
- Audit de sécurité des Systèmes d'informations
- Gestion des risques
- Politique de Sécurité du Système d'informations
- PSSIE
- Conclusion et perspectives

Introduction à la sécurité du SI

- **Gouvernance** : Ensemble de responsabilités et de pratiques qu'utilisent la direction d'une organisation pour fournir une orientation stratégique.
- De même Fournir l'assurance que :
  - les objectifs peuvent être atteints,
  - les risques sont gérés convenablement,
  - les ressources organisationnelles sont utilisées convenablement,
- On peut ajouter les relations entre les instances de décisions, les objectifs , les ressources, et la surveillance des résultats.

Audit de sécurité du SI

- **Audit des SI** : Examen formel, une entrevue ou un test des systèmes d'informations permettant de déterminer si:
  - les systèmes d'informations sont en conformité avec les lois, les règlements, les contrats ou les lignes directrices de l'industrie,
  - les données et les renseignements des Sis ont reçu les niveaux de confidentialité, d'intégrité et de disponibilité appropriés,
  - les ressources organisationnelles sont utilisées convenablement,
  - Les opérations de SI sont accomplies efficacement et les objectifs d'efficacité sont respectés

Processus d'Audit de sécurité du SI

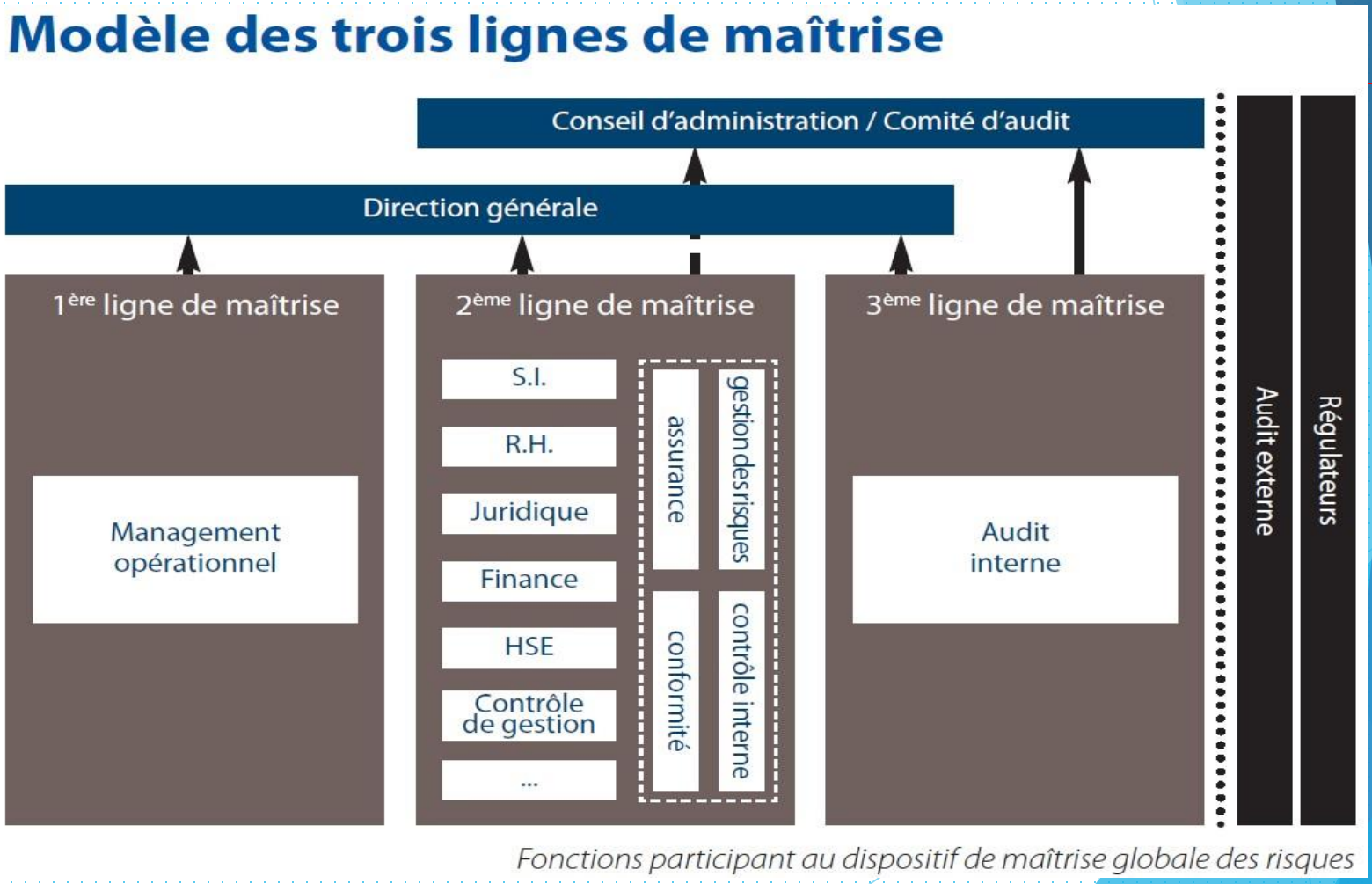
- **Le processus d'Audit** : elle traites des connaissances et des compétences nécessaire pour planifier et mener un audit
- **L'Audit des SI est axé sur le risque** : Interne et externe
- **la fonction d'audit** est gérée et dirigée de manière à assurer que les différentes tâches réalisées et exécutées par l'équipe d'audit répondent aux objectifs de la fonction d'audit;
- Indépendance de l'équipe doit être garantie

Processus d'Audit de sécurité du SI

- **Exécuter une stratégie d'audit des SI fondée sur le risque,** conforme aux normes d'audit des SI, pour assurer que les secteurs clés sont audités
- **Planifier des audits spécifiques** pour déterminer si les systèmes d'information sont protégés et contrôlés et s'ils apportent de la valeur à l'organisation
- **Effectuer les audits conformément aux normes d'audit des SI**
- pour attendre les objectifs d'audit planifiés
- **Communiquer les résultats et faire des recommandations** aux principales parties prenantes dans le cadre de réunions et de rapports d'audit pour promouvoir le changement au besoin.
- **Effectuer des suivis d'audits** pour déterminer si des mesures appropriées ont été prises par la direction de façon opportune

Processus d'Audit de sécurité du SI

L'organisation du dispositif d'audit interne



Processus d'Audit de sécurité du SI

- Gestion de la fonction d'audit des SI
- Normes et directives d'assurance et d'audit des si de l'ISACA
- Contrôles des SI
- Réaliser l'audit des SI
- Communiquer les résultats de l'audit
- Autoévaluation des contrôles
- Changements dans le processus d'audit

Processus d'Audit de sécurité du SI

- **L'organisation de la fonction d'audit:**
  - La charte d'audit,
  - la lettre de mission
- **Le management des ressources:**
  - Motivation
  - Formation
  - Outils

Processus d'Audit de sécurité du SI

- **Charte d'audit des SI** : Enoncer clairement les objectifs et responsabilités de la direction et de la délégation de pouvoir pour la fonction d'audit des SIs
- **La lettre de mission** : Met l'accent dur un exercice d'un audit particulier qui doit être exécuté dans une organisation pour atteindre un objectif spécifique

Types de Contrôles

Le contrôle constitue la boucle finale du processus de la gestion. Au regard des objectifs arrêtés dans le plan, le gestionnaire contrôle, en fin d'exercice, les résultats obtenus. Il apprécie le chemin fait et les performances réalisées.

- **Contrôles préventifs**: Le contrôle préventif permet de s'assurer que toutes les conditions et tous les paramètres nécessaires pour le fonctionnement de l'entreprise sont réunis
- **Contrôles défectifs**: Le contrôle a pour objectif de détecter si un risque s'est réalisé
- **Contrôles correctifs**: Le contrôle correctif se fait essentiellement à la fin d'un cycle ou d'une étape de la production. Au regard des résultats atteints et des normes établies dans le plan, le gestionnaire apporte les corrections qu'il juge indispensables pour mieux accomplir, durant l'exercice en cours ou pour la prochaine, les objectifs arrêtés
- **Contrôles compensatoire**: Procédure de contrôle mise en œuvre dans le but de contrebalancer les faiblesses du contrôle interne

Types de Contrôles

Le contrôle constitue la boucle finale du processus de la gestion. Au regard des objectifs arrêtés dans le plan, le gestionnaire contrôle, en fin d'exercice, les résultats obtenus. Il apprécie le chemin fait et les performances réalisées.

- **Contrôles préventifs**: Le contrôle préventif permet de s'assurer que toutes les conditions et tous les paramètres nécessaires pour le fonctionnement de l'entreprise sont réunis
- **Contrôles défectifs**: Le contrôle a pour objectif de détecter si un risque s'est réalisé
- **Contrôles correctifs**: Le contrôle correctif se fait essentiellement à la fin d'un cycle ou d'une étape de la production. Au regard des résultats atteints et des normes établies dans le plan, le gestionnaire apporte les corrections qu'il juge indispensables pour mieux accomplir, durant l'exercice en cours ou pour la prochaine, les objectifs arrêtés
- **Contrôles compensatoire**: Procédure de contrôle mise en œuvre dans le but de contrebalancer les faiblesses du contrôle interne

Gestion des risques

Objectifs de la gestion des risques:

- Comprendre l'importance de la gestion des risques en tant qu'outil pour répondre aux besoins de l'entreprise et développer un programme de gestion de la sécurité pour répondre à ces besoins
- Comprendre les moyens d'identifier, de classer et de répondre aux risques d'une manière appropriée telle que définie par les directives organisationnelles
- Évaluer la pertinence et l'efficacité des contrôles en matière de sécurité de l'information
- Etablir les rapports sur les risques de sécurité de l'information de manière efficace

Gestion des risques

Tâches et savoir faire:

T2.1 Établir et / ou maintenir un processus de classification des actifs informationnels afin de garantir que les mesures prises pour protéger les actifs sont proportionnelles à leur valeur commerciale.

T2.2 Identifier les exigences légales, réglementaires, organisationnelles et autres applicables pour gérer le risque de non-conformité à des niveaux acceptables.

T2.3 Veiller à ce que les évaluations des risques, les évaluations de la vulnérabilité et les analyses des menaces soient menées de manière cohérente et au moment opportun pour identifier et évaluer les risques pour les informations de l'organisation.

T2.4 Identifier, recommander ou mettre en œuvre des options appropriées de traitement / réponse aux risques pour gérer le risque à des niveaux acceptables en fonction de l'appétence au risque de l'organisation.

T2.5 Déterminer si les contrôles de sécurité de l'information sont appropriés et gèrent efficacement les risques à un niveau acceptable.

Gestion des risques

Tâches et savoir faire:

T2.6 Faciliter l'intégration de la gestion des risques liés à l'information dans les processus opérationnels et informatiques (p. Ex., Développement de systèmes, approvisionnement, gestion de projet) pour permettre un programme cohérent et complet de gestion des risques liés à l'information dans toute l'organisation.

T2.7 Surveiller les facteurs internes et externes (par exemple, le paysage des menaces, la cybersécurité, les changements géopolitiques, réglementaires) qui peuvent nécessiter une réévaluation des risques pour s'assurer que les changements aux scénarios de risque existants ou nouveaux sont identifiés et gérés de manière appropriée.

T2.8 Signaler la non-conformité et les autres changements dans le risque d'information pour faciliter le processus de prise de décision en matière de gestion des risques.

T2.9 Veiller à ce que les risques liés à la sécurité de l'information soient signalés à la haute direction pour permettre de comprendre l'impact potentiel sur les buts et objectifs de l'organisation.

Gestion des risques

- **Le risque** peut être défini comme la combinaison de la probabilité d'un événement et de ses conséquences. La probabilité d'un événement est la probabilité qu'une menace donnée exploite une vulnérabilité exposée. S'il n'y a pas de conséquences ou d'impact, on considère qu'il n'y a pas de risque. À l'inverse, plus les conséquences ou l'impact sont importants, plus le risque est grand.
- **L'exposition**, ou la mesure dans laquelle une vulnérabilité est exposée, à une menace est également prise en compte dans l'équation du risque puisque l'étendue de l'exposition affecte la probabilité de compromission (c'est-à-dire qu'une exposition moindre entraîne moins de probabilité ou de fréquence de compromis, réduisant ainsi le risque).
- L'exposition est également appelée surface d'attaque. Elle est affectée par l'étendue et l'efficacité des contrôles et par l'emplacement d'un périphérique particulier dans un réseau (c'est-à-dire qu'un serveur situé au milieu du réseau est susceptible d'être moins exposé aux attaques qu'un serveur du périmètre).

Gestion des risques

- La classification des actifs en fonction de leur valeur est un élément essentiel d'une gestion efficace des risques car plus la valeur est élevée, plus l'impact potentiel est grand et, par conséquent, plus le risque est grand.
- La valeur est une combinaison de criticité des opérations et / ou de sensibilité, qui est fonction des dommages possibles à l'organisation résultant d'une divulgation non autorisée (par exemple, plans stratégiques, listes de clients). Comme il est prudent de protéger davantage les actifs informationnels de grande valeur, la gestion la plus rentable du risque informationnel peut être obtenue en allouant des ressources de protection proportionnellement à la valeur. La tâche consiste à développer un schéma de classification qui optimise cette allocation ainsi que les critères par lesquels ces ressources peuvent être efficacement classées.

Gestion des risques

- Une fois qu'un risque a été identifié, analysé et évalué pour déterminer s'il répond aux critères d'acceptabilité, les options de traitement (ou de réponse) doivent être analysées. Les choix disponibles comprennent l'acceptation du risque, le transfert du risque, l'arrêt de l'activité créant le risque (éviter) ou l'atténuation du risque. Les coûts et les conséquences potentielles de chacune des options doivent être pris en compte. Si des contrôles d'atténuation sont choisis parce que le risque dépasse l'appétit pour le risque de l'organisation, alors les options d'atténuation et la rentabilité doivent être évaluées. De plus, le risque de contrôle des options possibles de réduction des risques doit également être déterminé (c'est-à-dire le risque que le contrôle échoue ou soit inadéquat).
- L'efficacité du contrôle change généralement avec le temps à mesure que le risque évolue.
- Par conséquent, il est essentiel de tester et d'évaluer périodiquement si les contrôles existants continuent d'être efficaces et répondent toujours aux objectifs de contrôle. Les contrôles de test nécessiteront généralement de simuler les conditions auxquelles le contrôle est censé répondre, comme cela est fait dans les tests de pénétration.

Gestion des risques

- Le paysage des risques évolue constamment avec de nouvelles menaces, de nouvelles réglementations, de nouvelles modalités d'attaque et des vulnérabilités en constante évolution. Le responsable de la sécurité de l'information surveille l'évolution de la situation pour éviter d'exposer l'organisation à des risques accrus. Les sources publiques d'information sur les menaces externes doivent être régulièrement examinées.
- Les changements internes doivent également être surveillés en permanence; certains peuvent être suivis à travers le processus de contrôle des changements, mais d'autres aspects doivent être surveillés par des métriques, des rapports, des audits ou une observation directe.

Gestion des risques

- La gestion des risques est un processus visant à atteindre un équilibre optimal entre la réalisation des opportunités de gain et la minimisation des vulnérabilités et des pertes. Ceci est généralement accompli en s'assurant que l'impact des menaces exploitant les vulnérabilités se situe dans des limites acceptables à un coût acceptable.
- En termes pratiques, la gestion des risques signifie que les risques sont gérés de manière à ne pas avoir d'incidence importante sur le processus opérationnel de manière défavorable et qu'un niveau acceptable d'assurance et de prévisibilité des résultats souhaités de toute activité organisationnelle importante est prévu. Le risque est inhérent à toutes les activités; En règle générale, un niveau de risque stratégique plus élevé sera pris pour tenter d'obtenir des rendements plus élevés.
- La base d'une gestion efficace des risques est une évaluation complète des risques, fondée sur une solide compréhension de l'univers des risques de l'organisation. Il n'est pas possible d'élaborer un programme de gestion des risques pertinent si l'on ne comprend pas la nature et l'étendue du risque pour les ressources d'information et l'impact potentiel sur les activités de l'organisation

Gestion des risques

Le responsable de la sécurité de l'information doit également comprendre que la gestion des risques doit opérer à plusieurs niveaux, y compris les niveaux stratégique, de gestion et opérationnel. L'importance de l'expérience commerciale et de la prise de décision commerciale dans tout processus d'évaluation des risques doit être reconnue comme importante pour obtenir des résultats réalistes et réussis du processus. La probabilité et la pertinence d'une menace ou d'un risque particulier sont généralement une question de jugement, de sorte que l'expérience est bénéfique pour arriver à des résultats réalistes. Une bonne pratique consiste à signaler à la fois les résultats probables et les pires situations.

Stratégie de gestion des risques

Une stratégie de gestion des risques est le plan pour atteindre les objectifs de gestion des risques. En fin de compte, ces objectifs sont d'atteindre un niveau de risque acceptable dans l'ensemble de l'entreprise, ce qui entraîne un niveau acceptable de perturbation des activités de l'organisation.

Le niveau de risque acceptable est une décision de gestion généralement fondée sur une variété de facteurs, notamment:

- La capacité de l'organisation à absorber les pertes
- Coûts pour atteindre des niveaux de risque acceptables
- Rapports risques-avantages

Le risque acceptable détermine les objectifs de contrôle, qui deviennent les principaux objectifs de la stratégie.

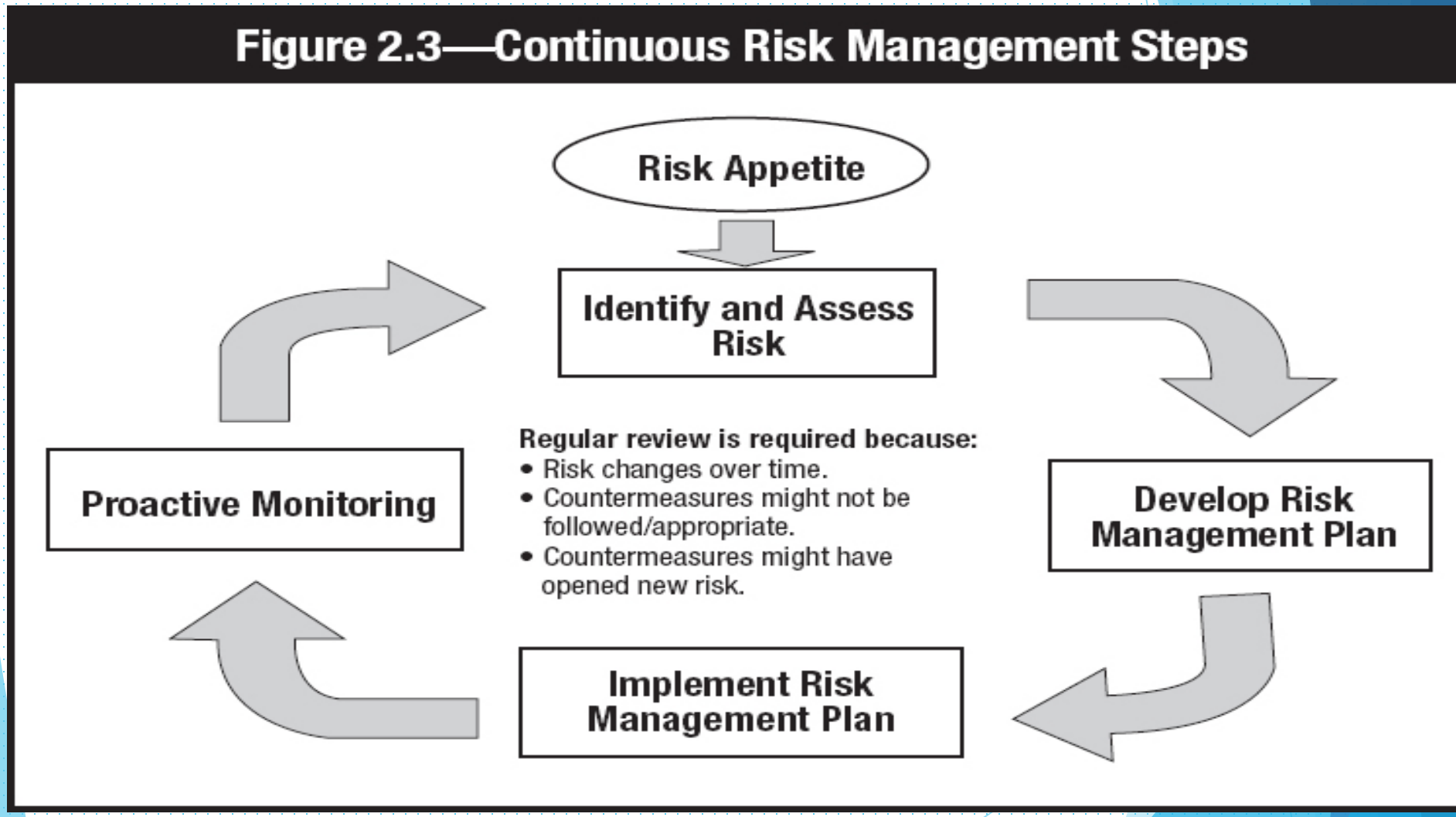
Pour être efficace et garantir une gestion cohérente des risques dans l'ensemble de l'entreprise, il est essentiel que la stratégie de gestion des risques liés à l'information soit intégrée aux autres activités de gestion des risques de l'organisation. Il s'agit d'éviter les lacunes de protection et la duplication des efforts et garantira que les diverses activités de gestion des risques ne fonctionnent pas à contre-courant.

Programme de gestion de risques

Les étapes initiales de l'élaboration d'un programme de gestion des risques comprennent :

- **Contexte et objectif du programme**
- **Portée et charte**
- **Autorité, structure et relations hiérarchiques**
- **Identification, classification et propriété des actifs**
- **Objectifs de gestion des risques**
- **La méthodologie à utiliser**
- **L'équipe de mise en œuvre**

Processus de gestion des risques



Processus de gestion des risques

La gestion des risques consiste en une série de processus qui prennent en compte les exigences de bout en bout d'identification, d'analyse, d'évaluation et de maintien des risques à des niveaux acceptables. La gestion des risques comprend généralement les processus suivants:

- **Établir la portée et les limites** - Processus pour l'établissement de paramètres globaux pour la performance de la gestion des risques au sein d'une organisation. Les facteurs internes et externes doivent être pris en compte pour fournir le contexte.
- **Identifier les actifs informationnels et leur évaluation** - Un inventaire des actifs informationnels et un processus d'évaluation pour déterminer les actifs à risque et les impacts potentiels des compromis
- **Effectuer une évaluation des risques** - Un processus consistant en l'identification, l'analyse et l'évaluation des risques, notamment:

- Identifier les menaces, vulnérabilités et expositions viables
- Analyser le niveau de risque et l'impact potentiel
- Évaluer si le risque répond aux critères d'acceptation

Processus de gestion des risques

- **Déterminer le traitement du risque ou la réponse** - Processus de sélection des stratégies pour faire face au risque identifié qui dépasse le niveau acceptable. Le risque est généralement accepté s'il n'y a pas de moyen rentable de l'atténuer, s'il y a peu d'exposition ou d'impact potentiel, ou s'il n'est tout simplement pas possible de le traiter efficacement.

- **Accepter le risque résiduel** - La décision et l'approbation par la direction d'accepter le risque restant après la fin du processus de traitement, si nécessaire, (c'est-à-dire que le risque peut être accepté après que l'évaluation montre qu'il se situe dans des limites acceptables ou si aucune option de traitement efficace n'est disponible.)

- **Communiquer et surveiller les risques** Un processus permettant d'échanger et de partager des informations relatives aux risques, ainsi que d'examiner l'efficacité de l'ensemble du processus de gestion des risques.

Processus de gestion des risques

- **Déterminer le traitement du risque ou la réponse** - Processus de sélection des stratégies pour faire face au risque identifié qui dépasse le niveau acceptable. Le risque est généralement accepté s'il n'y a pas de moyen rentable de l'atténuer, s'il y a peu d'exposition ou d'impact potentiel, ou s'il n'est tout simplement pas possible de le traiter efficacement.

- **Accepter le risque résiduel** - La décision et l'approbation par la direction d'accepter le risque restant après la fin du processus de traitement, si nécessaire, (c'est-à-dire que le risque peut être accepté après que l'évaluation montre qu'il se situe dans des limites acceptables ou si aucune option de traitement efficace n'est disponible.)

- **Communiquer et surveiller les risques** Un processus permettant d'échanger et de partager des informations relatives aux risques, ainsi que d'examiner l'efficacité de l'ensemble du processus de gestion des risques.

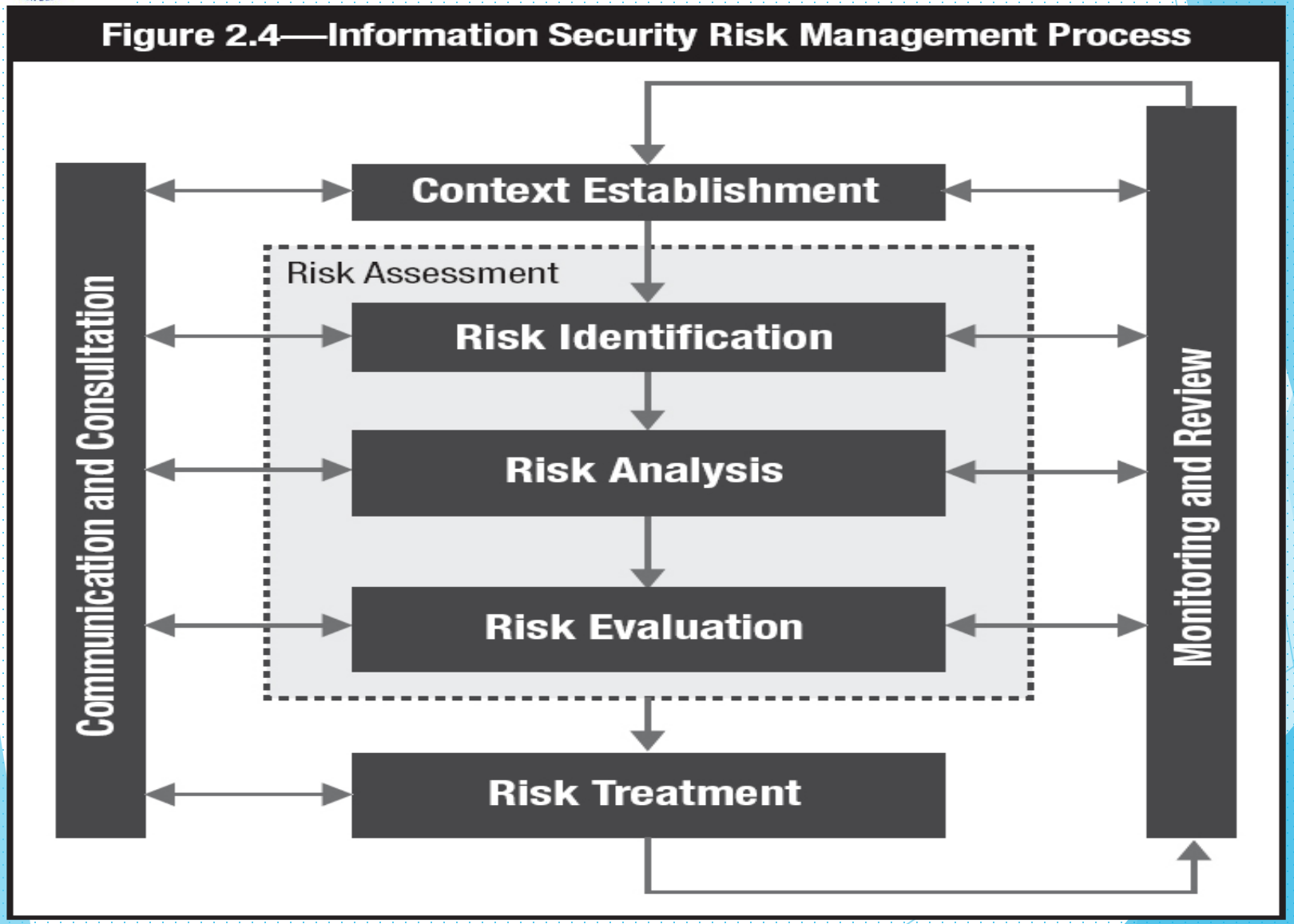
Notions de gestion des risques

L'appétence au risque est ce que la direction considère comme un niveau de risque acceptable, et la tolérance au risque est le niveau acceptable d'écart par rapport au niveau de risque acceptable. L'appétence au risque est une décision basée sur un certain nombre de critères notamment les considérations réglementaires, la capacité à absorber les pertes, les problèmes de réputation, la mission et la culture.

Quelques autres notions :

- Objectifs de temps de récupération (RTO)
- Objectifs de point de récupération (RPO)
- Redondance
- Évaluation des ressources
- Reporting des risques
- Tolérance au risque
- Traitement des risques et réponse
- Fenêtre d'interruption acceptable (AIW)
- Analyse d'impact sur l'entreprise (BIA)
- Contrôles
- Contre-mesures
- Criticité
- Exposition
- La fréquence
- Impacts
- Classification des actifs informationnels
- Indicateurs de risque clés (KRI)
- Indisponibilité maximale tolérable (MTO

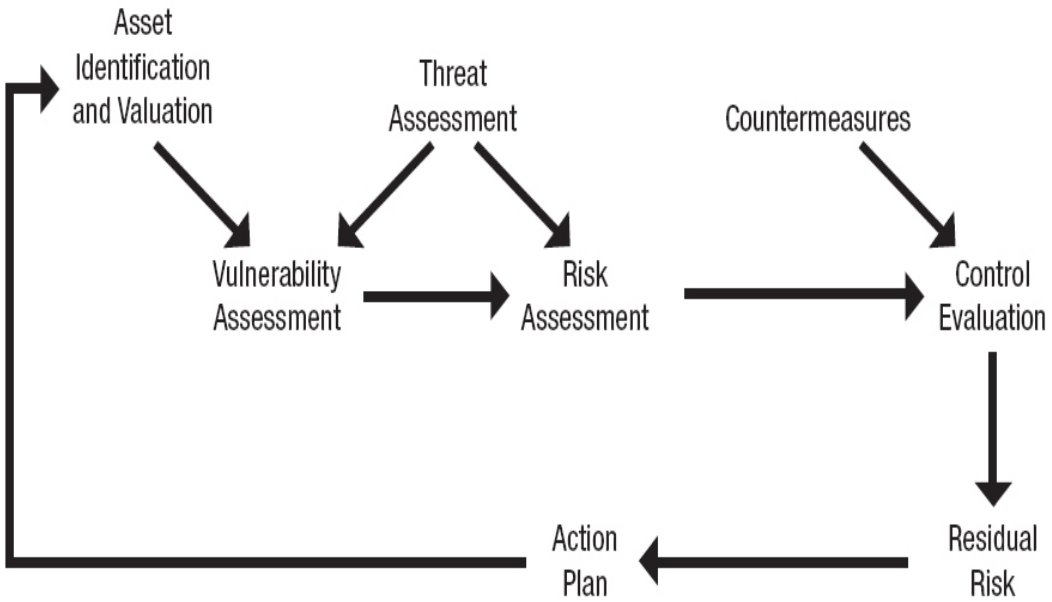
Evaluation et Analyse de risques



Source: ISACA, COBIT 5 for Risk, USA, 2013, figure 47

Evaluation et Analyse de risques

Figure 2.5—Risk Analysis Framework



Source: ISACA, *IT Governance Implementation Guide, 2nd Edition-Supplemental Tools and Materials*, CD-ROM, USA, 2007

Evaluation et Analyse de risques

La plupart des approches d'évaluation des risques comportent quartes phases:

- ***L'identification des risques*** est le processus qui consiste à utiliser des scénarios de risque pour déterminer l'étendue et la nature des risques pour l'organisation.

- ***L'analyse des risques*** est le processus qui consiste à combiner les informations de vulnérabilité recueillies et les informations sur les menaces recueillies auprès d'autres sources pour déterminer le risque de compromission en termes de fréquence et d'ampleur potentielle. L'analyse peut inclure des éléments comme l'espérance de perte annualisée (ALE).

- ***L'évaluation des risques*** est le processus consistant à comparer les résultats de l'analyse des risques aux critères établis d'acceptabilité, d'impact, de probabilité et de nécessité d'un traitement supplémentaire.

- **Le monitoring et reporting des risques.**

PSSI : Politique de sécurité du SI

La gouvernance de la sécurité du système d'information implique d'assurer le développement de procédures et de directives qui supportent la politique de sécurité de l'information:

La rédaction de procédures est différente de la rédaction de politiques en ce qu'il n'est pas utile de demander aux équipes de développer les procédures.

Les procédures ne devront pas être approuvées par une équipe de gestion. Le processus est plus rapide, tout en nécessitant un peu de travail•

PSSI : Politique de sécurité du SI

A ce titre le Benin a adopté:

- Stratégie Nationale de Sécurité Numérique (SNSN)
- Politique de Sécurité des Systèmes d'Information de l'État (PSSIE)
- Guide des bonnes pratiques de sécurité du télétravailleur
- Livre Blanc : Règles d'hygiène de base pour une sécurité numérique personnelle améliorée

PSSI : Politique de sécurité du SI

- La PSSIE est conçu à base des référentiels internationaux, tel que: la norme ISO/CEI 27001: 2013 ainsi que la norme ISO/CEI27005 de management des risques
- Les questionnaires de l'audit sont basés sur vingt trois (23) domaines que couvre la politiques de sécurité du système d'information de l'état
- Les Règles et Recommandations pour chaque exigence spécifique sont définies dans la PSSIE :*
- Du Domaine n◦ 1, Organisation de la sécurité des SI en passant par le Domaine n◦ 2, Sécurité des ressources humaine….jusqu'au Domaine n◦ 23, Conformité, audit et contrôles de sécurité.
- Des objectifs via la mise en oeuvre des contrôles et des exigences ont été formulées

Merci de votre attention