

Technologies de l'information

Cours:

**Sécurité des systèmes
informatiques**

Séance # 5

Préparé par: Blaise Arbouet



DESS

Retour sur la séance 4 concernant la gestion de risque

Etape 2: Identification du risque

- Mesures existantes (collecte et évaluation)
- Les vulnérabilités (types et sources)
- Identification des conséquences (évaluation et critères)

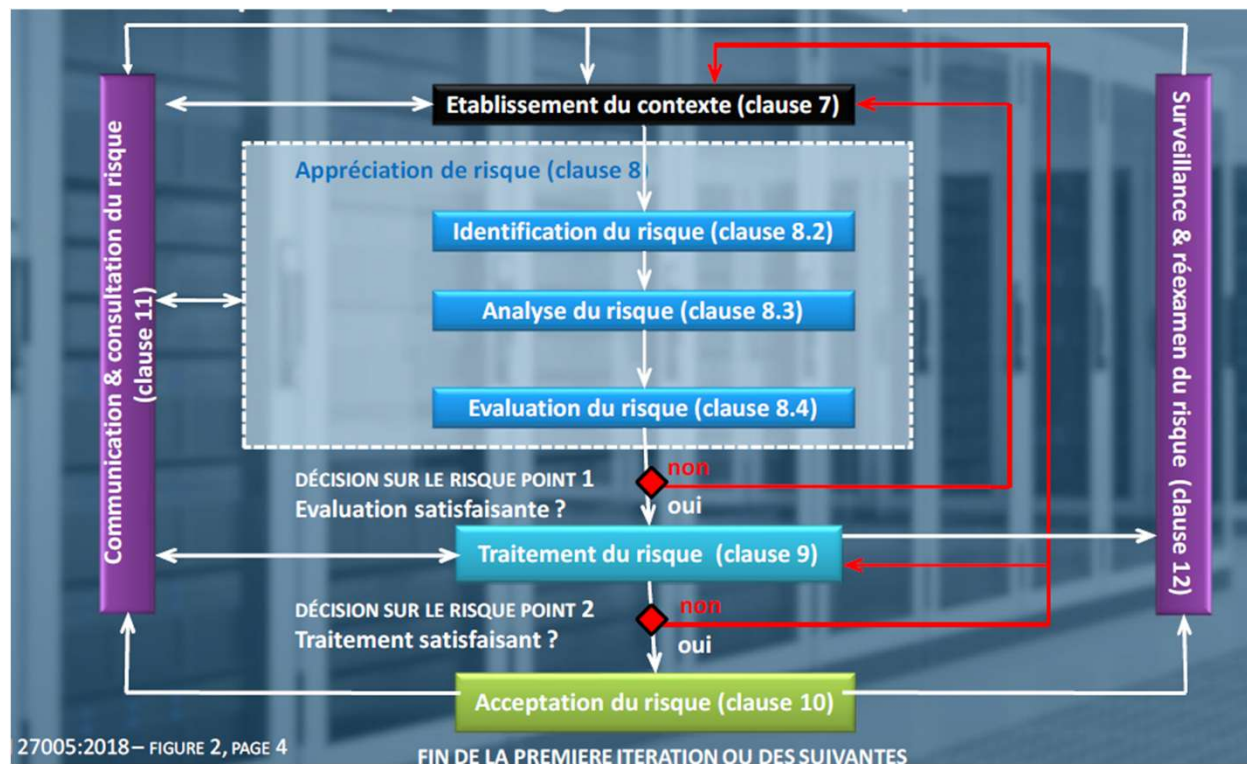
Etape 3: Analyse de risques

- Approche quantitative et qualitative
- Appréciation de la probabilité et de l'impact.

Etape 4: Évaluation de risques

- Priorisation des scénarios
- Niveau de gravité

Processus de gestion de risque avec ISO 27005



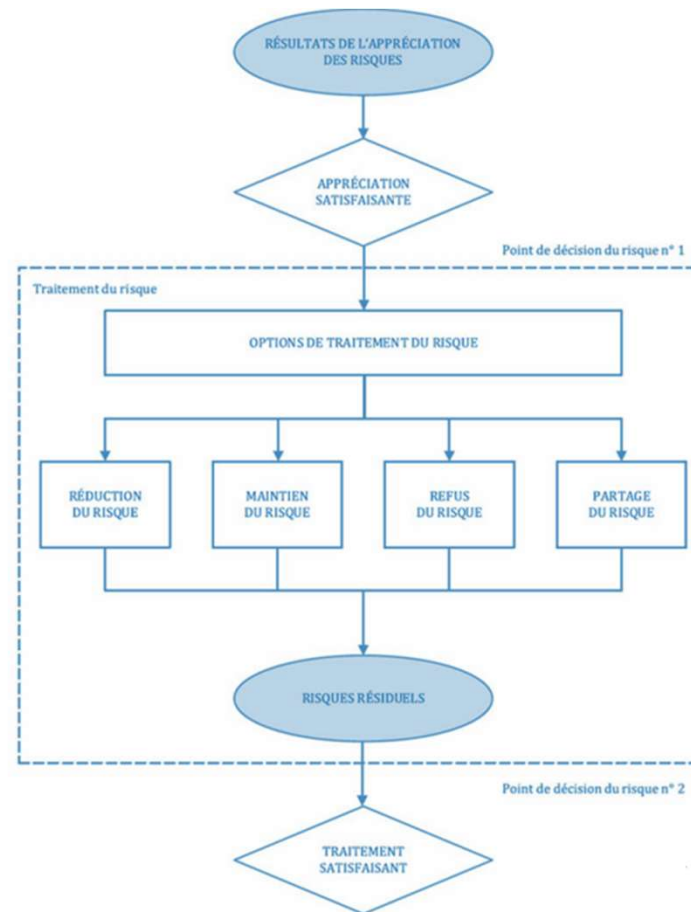
Étape 5

Traitement des risques

Traitement des risques

Quatre options de traitement des risques sont possibles:

- la réduction du risque
- le maintien (acceptation) du risque
- le refus du risque
- le partage (transfert) du risque

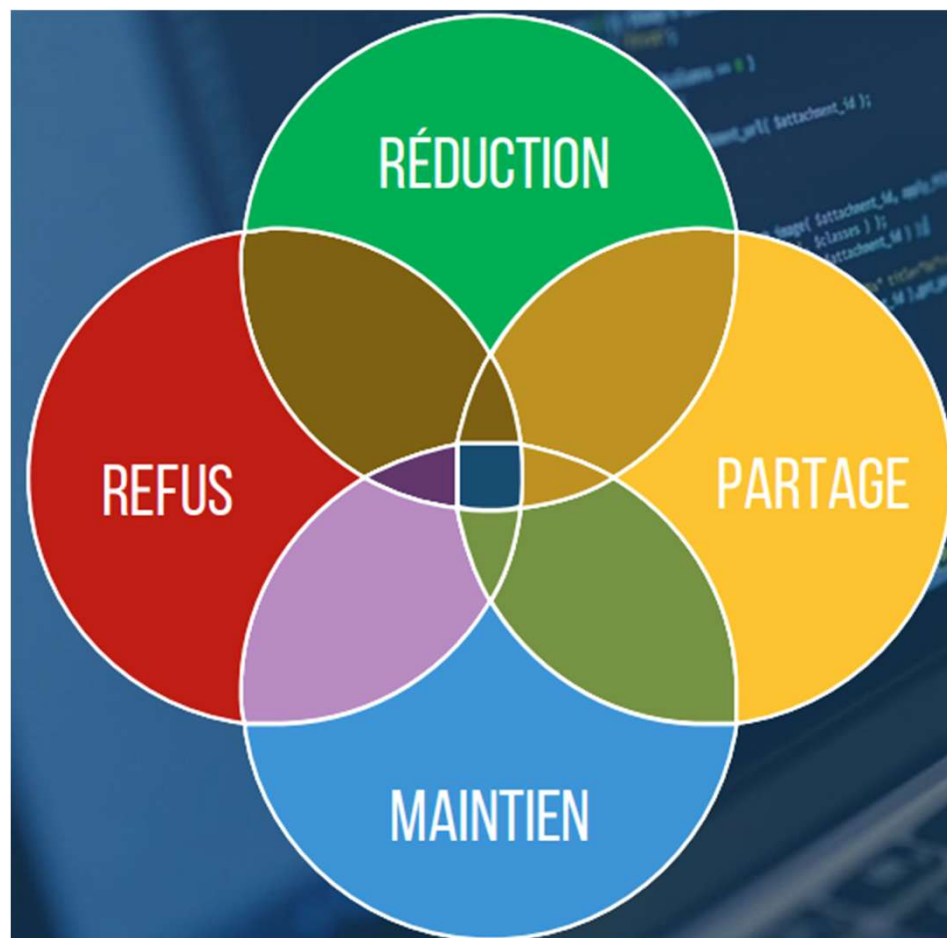


Sélection des options de traitement

Il convient de choisir les options de traitement sur la base des résultats de l'appréciation des risques, du coût prévu de mise en œuvre ainsi que des bénéfices attendus.

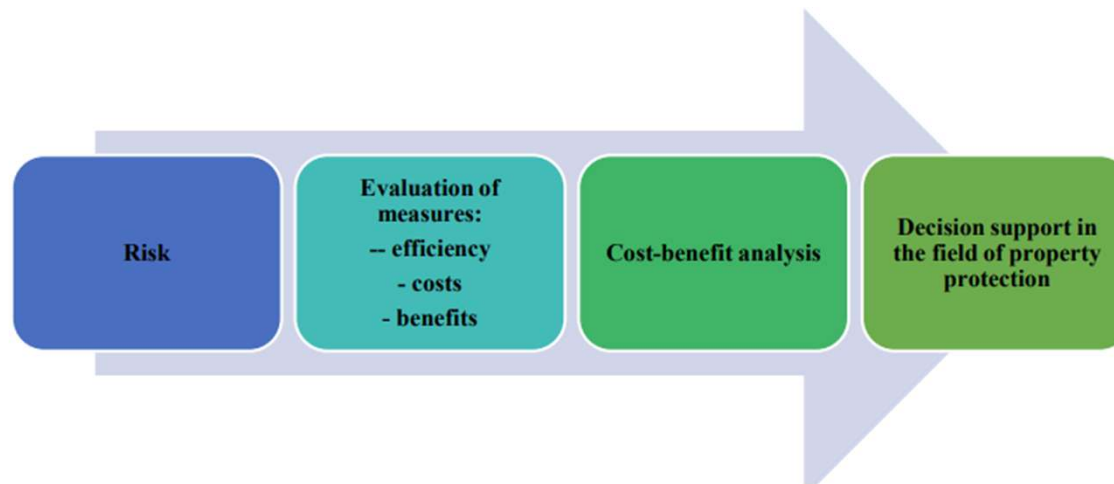
Les quatre options relatives au traitement des risques ne s'excluent pas mutuellement.

L'organisme peut parfois retirer des bénéfices substantiels d'une combinaison d'options.



Analyse coûts/bénéfices et priorité de traitement

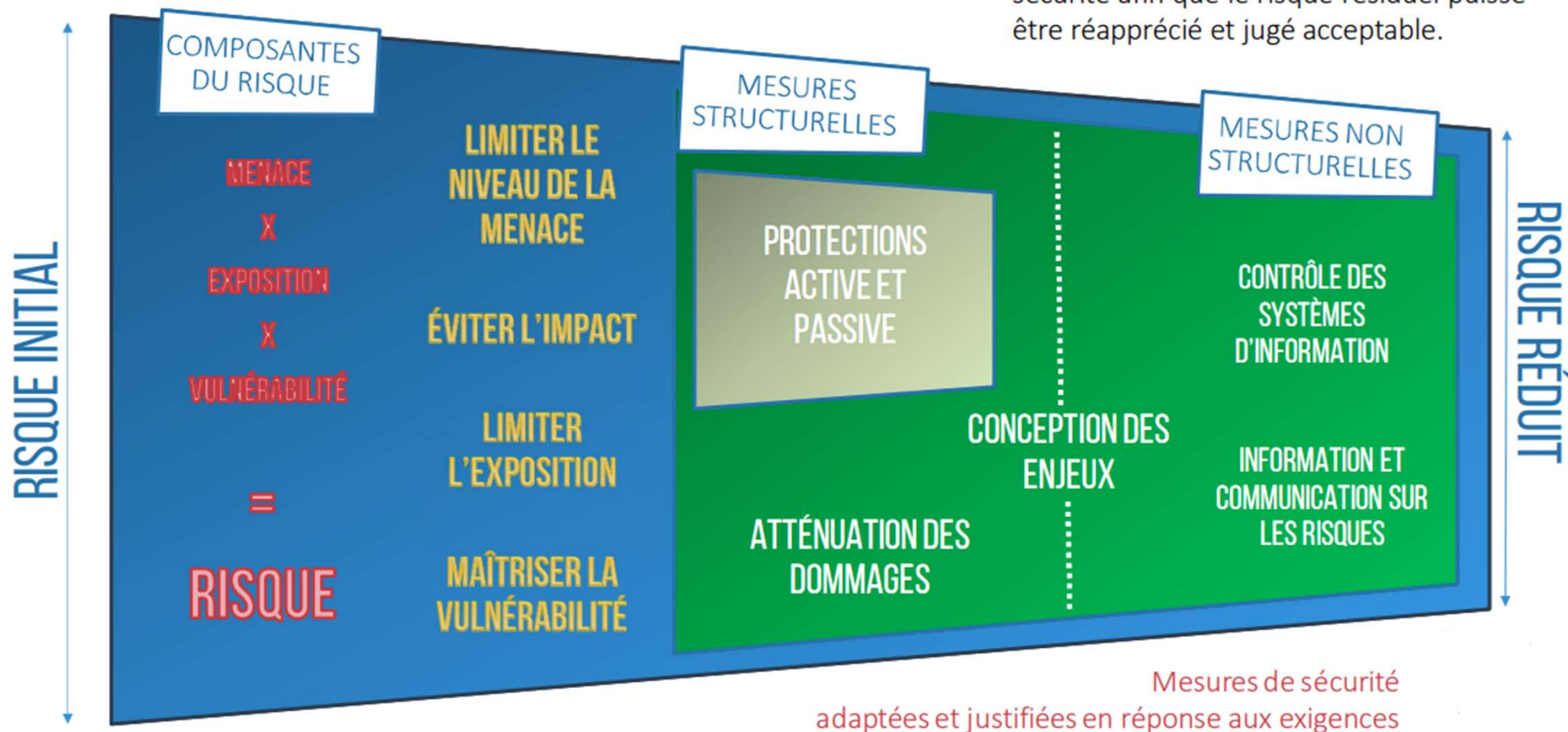
Il est de la responsabilité des dirigeants d'équilibrer les coûts de mise en œuvre des mesures de sécurité et l'attribution de budgets.



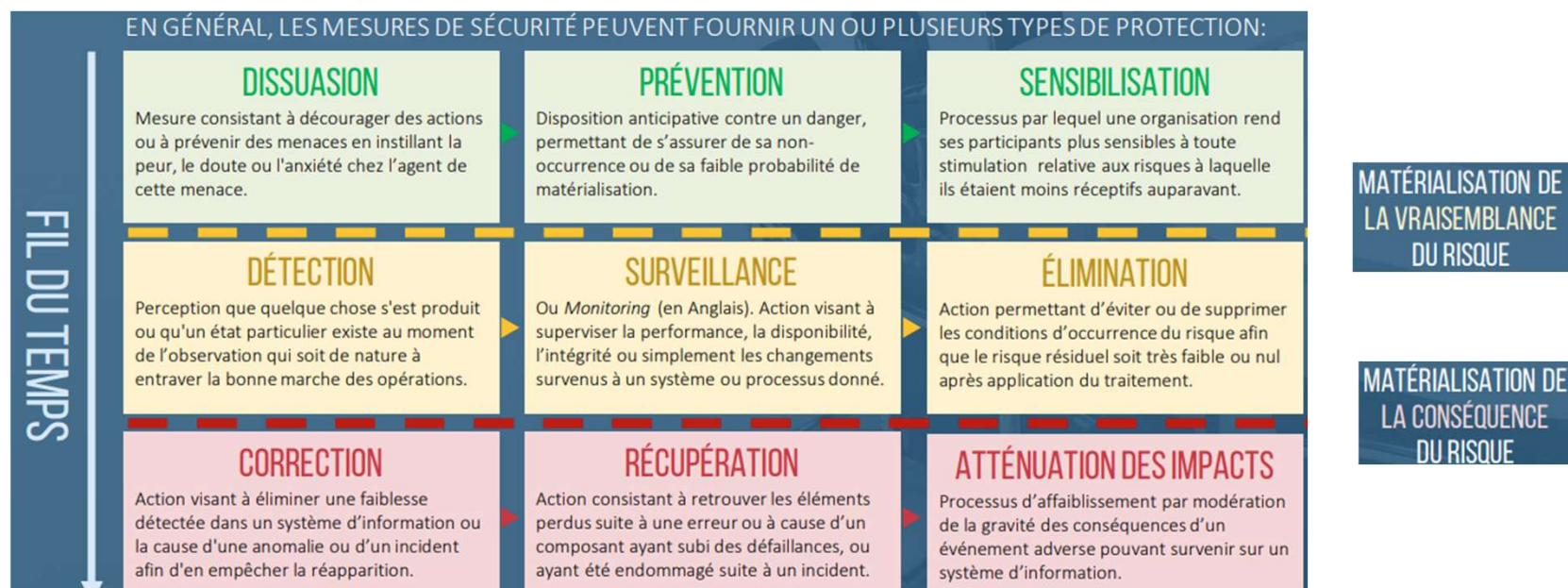
Source: Le processus d'une analyse cout avantage pour la protection d'une propriété.

Réduction du risque

Il convient de réduire le niveau des risques par l'introduction, la suppression ou la modification des mesures de sécurité afin que le risque résiduel puisse être réapprécié et jugé acceptable.



Type de mesures de sécurité



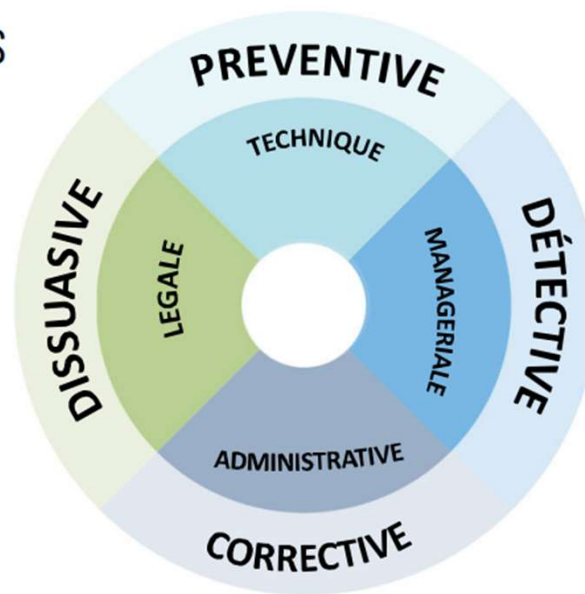
Nature et catégorie des mesures

4 NATURES DE MESURES

- Dissuasive
- Préventive
- Détective
- Corrective

4 CATÉGORIES DE MESURES

- Technique
- Managériale
- Administrative
- Légale



35 OBJECTIFS DE SÉCURITÉ DANS LE SMSI

Déclaration qui décrit ce qui doit être mis en place suite à l'implantation des mesures de sécurité dans le système d'information.

114 MESURES DE SÉCURITÉ (ANNEXE A)

- Disposition de modification des risques
- Elles incluent toutes les actions qui modifient la vraisemblance d'apparition ou la gravité des conséquences des risques en sécurité de l'information
- Elles ne permettent pas toujours d'obtenir le résultat escompté.

Natures principales de mesure de sécurité

- **Dissuasive** : ce type de contrôle est difficile à quantifier. Le but d'un contrôle dissuasif c'est de réduire la probabilité de vulnérabilités qui sont exploitées sans réellement réduire la visibilité.
- **Préventive** : Toutes les mesures prises avant une urgence, une perte ou un problème qui survient. Elles incluent l'utilisation d'alarmes et de serrures, la sélection des autorisations (pour empêcher les enregistreurs de cash de contrôler l'argent et le personnel responsable des stocks de contrôler l'inventaire) ainsi que d'autres politiques d'autorisation générales et spécifiques.
- **Détective** : Utilisé pour détecter les attaques contre les systèmes d'information et les empêcher de réussir. Les contrôles de type détectif sont aussi désignés pour contrôler les pannes de matériel ou du système et fournir des alertes adéquates aux administrateurs du système pour empêcher les interruptions du système.
- **Corrective** : Il s'agit en premier lieu de réduire l'Impact d'une vulnérabilité exploitée plutôt que de prévenir son apparition. Le point clé ici est que l'attaque a déjà commencé et tout ce qu'on peut faire c'est limiter sa sévérité. Le but du contrôle correctif devrait être de réduire la quantité de processus matériels ou d'actifs d'informations qui sont exposés.

Catégories principales de contrôles

Technique : les contrôles liés à l'utilisation de mesures techniques ou de technologies telles que les firewalls, systèmes d'alarme, caméras de surveillance, intrusion systèmes de détection (IDS), etc.

Administratif / Managérial : les contrôles liés à la structure organisationnelle telle que la sélection des autorisations, la rotation des métiers, les descriptions de métier, les processus d'approbation, le management des revues et des audits.

Légal : Les contrôles liés aux applications des exigences légales et réglementaires ou des obligations contractuelles Les différences entre les catégories de contrôles de sécurité sont expliquées seulement pour une meilleure compréhension. Aucune entreprise ne doit évaluer la catégorie de contrôle de sécurité qui doit être installé.

Enjeux et contraintes liés aux mesures de sécurité

De nombreuses contraintes existent et qui sont susceptibles d'affecter le choix des mesures de sécurité.

Ces contraintes peuvent empêcher l'utilisation de certaines mesures de sécurité, ou peuvent **provoquer des erreurs humaines** annulant la mesure de sécurité, ou peuvent provoquer des erreurs humaines annulant la mesure de sécurité, en créant **une fausse impression de sécurité**, ou même en augmentant le risque au-delà de la **non mise en œuvre de la mesure de sécurité** (par exemple, en exigeant des mots de passe complexes sans réelle formation, poussant ainsi les utilisateurs à écrire leur mot de passe sur papier). De plus, une mesure de sécurité peut toujours **altérer les performances**.

Recommandations des mesures de sécurité

Les mesures de sécurité sont testées avant leur mise en oeuvre

Les personnes sont formées à l'utilisation des mesures

Un propriétaire est identifié pour chaque mesure

Le résultat de la mesure est effectivement mesurable

Les mesures sont documentées de manière claire

L'efficacité des mesures est surveillée dans le temps

Exemple de réduction du risque

MENACE	VULNÉRABILITÉ	ACTIFS CONCERNÉS	RISQUE
Défaillance système : Surchauffe dans la salle des serveurs.	Le système de climatisation a 10 ans.	<ul style="list-style-type: none">▪ Bases de données▪ Fichiers site web▪ Serveurs physiques▪ Câblage réseau	Perte potentielle : 75.000 € par occurrence
Niveau de menace : ÉLEVÉ (4/5)	Niveau de vulnérabilité : ÉLEVÉ (4/5)	Valeur de l'actif : CRITIQUE (5/5)	Niveau de risque : TRÈS ÉLEVÉ (20/25)

La température de la salle de serveurs est déjà de 40 °C. Il y a eu 2 pointes à 57°C en un an.

TRÈS PROBABLE (4/5)

Tous les services (applications SaaS, site web, messagerie, etc.) seront indisponibles pendant au moins deux mois.

TRÈS ÉLEVÉ (5/5)

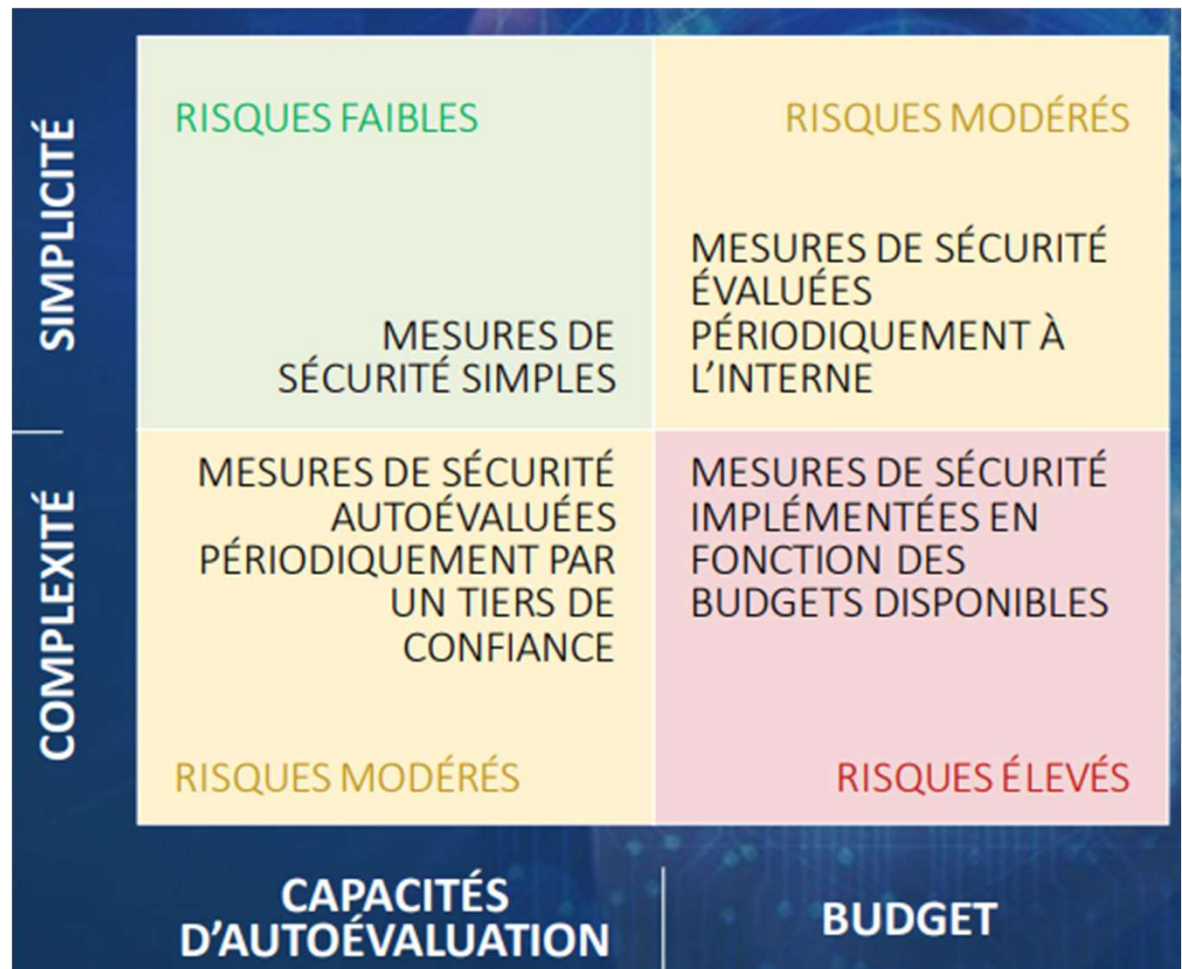
RÉDUIRE LE RISQUE PAR UNE MESURE TECHNIQUE PRÉVENTIVE

Achat et installation d'un nouveau système de climatisation pour la salle des serveurs.

- Étude : 7.000 €
 - Matériel : 33.000 €
 - Installation : 5.000 €
 - Maintenance 10 ans : 25.000 €
- } 45.000€/setup
+
2.500€/an

Maintien ou acceptation du risque

Si le niveau des risques répond aux critères d'acceptation des risques, il n'est pas nécessaire de mettre en oeuvre d'autres mesures de sécurité, le risque peut alors être conservé.



Exemple de maintien du risque

MENACE	VULNÉRABILITÉ	ACTIFS CONCERNÉS	RISQUE
Interférence humaine involontaire par suppression accidentelle de fichiers.	Autorisations correctement configurées, logiciel d'audit en place, sauvegardes régulières et testées.	Fichiers publics et à usage interne, stockés sur un partage de fichiers Windows.	Perte potentielle : Temps de travail d'un opérateur de backup pour restaurer les fichiers accidentellement détruits
Niveau de menace : MOYEN (3/5)	Niveau de vulnérabilité : FAIBLE (1/5)	Valeur de l'actif : MOYEN (2/5)	Niveau de risque : FAIBLE (6/25)

Ce cas se produit plusieurs fois par mois. **PROBABLE (3/5)**

Perte de données critiques mais celles-ci pourront certainement être restaurées depuis une sauvegarde. **MOYEN (2/5)**

MAINTENIR LE RISQUE VIA LA MESURE MANAGÉRIALE DÉTECTIVE

Continuer à surveiller les modifications apportées aux autorisations, les utilisateurs privilégiés et les sauvegardes

- Aucun coût supplémentaire



ABANDONNER

Il est possible de prendre la décision d'éviter complètement le risque, en abandonnant une ou plusieurs activités prévues ou existantes, ou en modifiant les conditions dans lesquelles l'activité est effectuée.



CHANGER DE STRATÉGIE

Pour les risques découlant d'incidents naturels, il peut être plus rentable de déplacer physiquement les moyens de traitement de l'information à un endroit où le risque n'existe pas ou est maîtrisé.

Partage ou transfert du risque

Partage des risques

ISO 27005, Clause 9.5



Il convient de partager le risque avec une autre partie capable de gérer de manière plus efficace le risque spécifique en fonction de l'évaluation du risque.

PARTAGE DES RISQUES

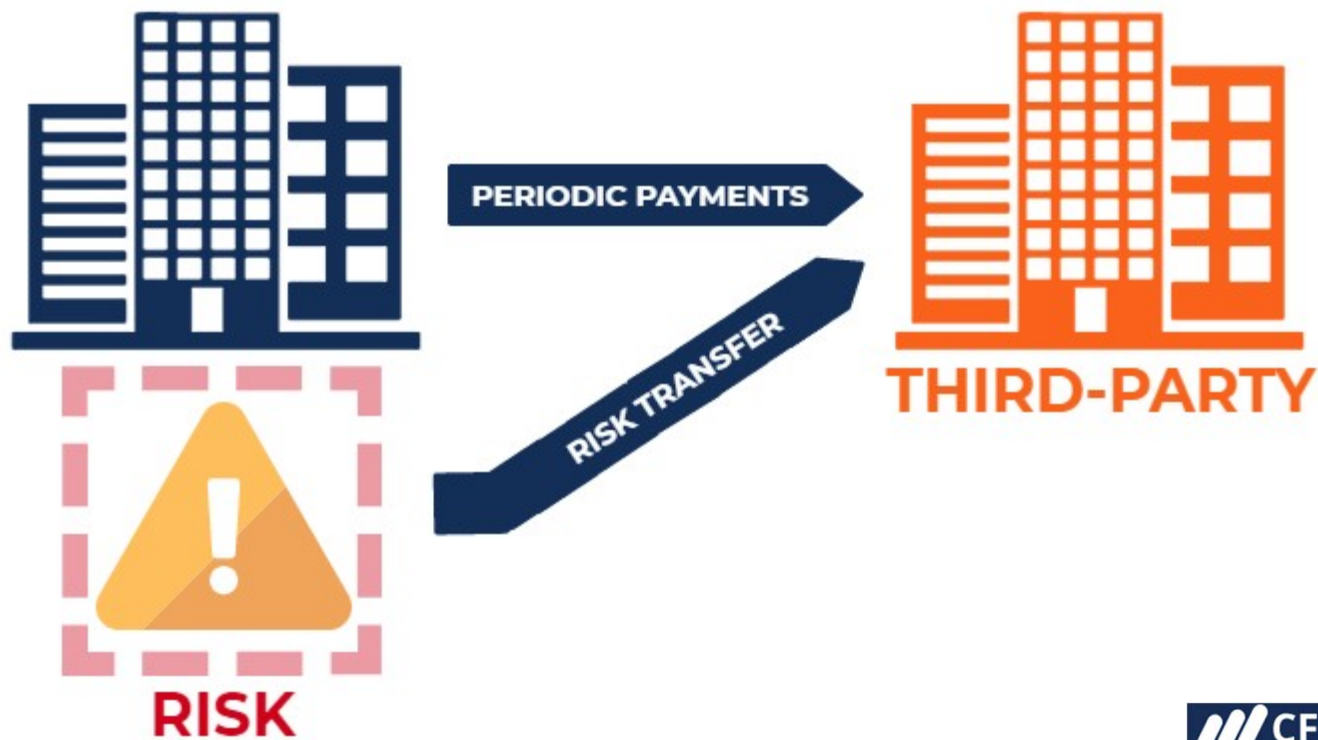


Ce partage peut être envisagé avec l'aide active d'une tierce partie dont le rôle consiste à prendre en charge une partie de la responsabilité, opérationnelle ou financière.

EXEMPLE DE PARTAGE DE RISQUE

MENACE	VULNERABILITÉ	ACTIFS CONCERNÉS	RISQUE
Panne de système: Disque dur inopérant	Il n'y a pas de sauvegarde des données	Plateforme e-commerce Fichiers clients Catalogue de produits Baie de stockage	Perte potentielle: 100,000\$ par occurrence
Niveau de la menace: Élevé (4/5)	Niveau: Elevé (4/5)	Valeur de l'actif: Critique (5/5)	Niveau: Très Elevé (20/25)
Probabilité		Impact	
Possible (4/5)		Très élevé (5/5)	
La baie de stockage est récente et n'a pas de redondance		Perte de toutes les données clients	
Mesure de traitement du risque		Coût de la mesure	
Partager le risque par une mesure technique préventive		Abonnement à une formule cloud	
Sauvegarde quotidienne chez un fournisseur infonuagique		69 \$ par mois	

Transfert de risque par l'achat une cyber-assurance



Partage des risques

Aspects de responsabilité

RESPONSABILITÉ EN GESTION DES RISQUES

Il est possible de partager la responsabilité de la gestion des risques.

RESPONSABILITÉ LÉGALE

Il est en revanche impossible de transférer la responsabilité légale d'un impact.



LES CLIENTS
ATTRIBUENT GÉNÉRALEMENT À L'ORGANISME
LA RESPONSABILITÉ D'UN EFFET INDÉSIRABLE.

Plan de traitement des risques

[illegible]

Détermination des risques résiduels



RISQUES INACCEPTABLES

Le risque doit être réduit indépendamment des coûts à moins que des circonstances extraordinaires ne s'appliquent ou que la Direction ne décide de l'accepter (voir section suivante)

RISQUES TOLÉRABLES

Le risque est tolérable seulement si toutes les étapes raisonnables ont été entreprises pour le réduire

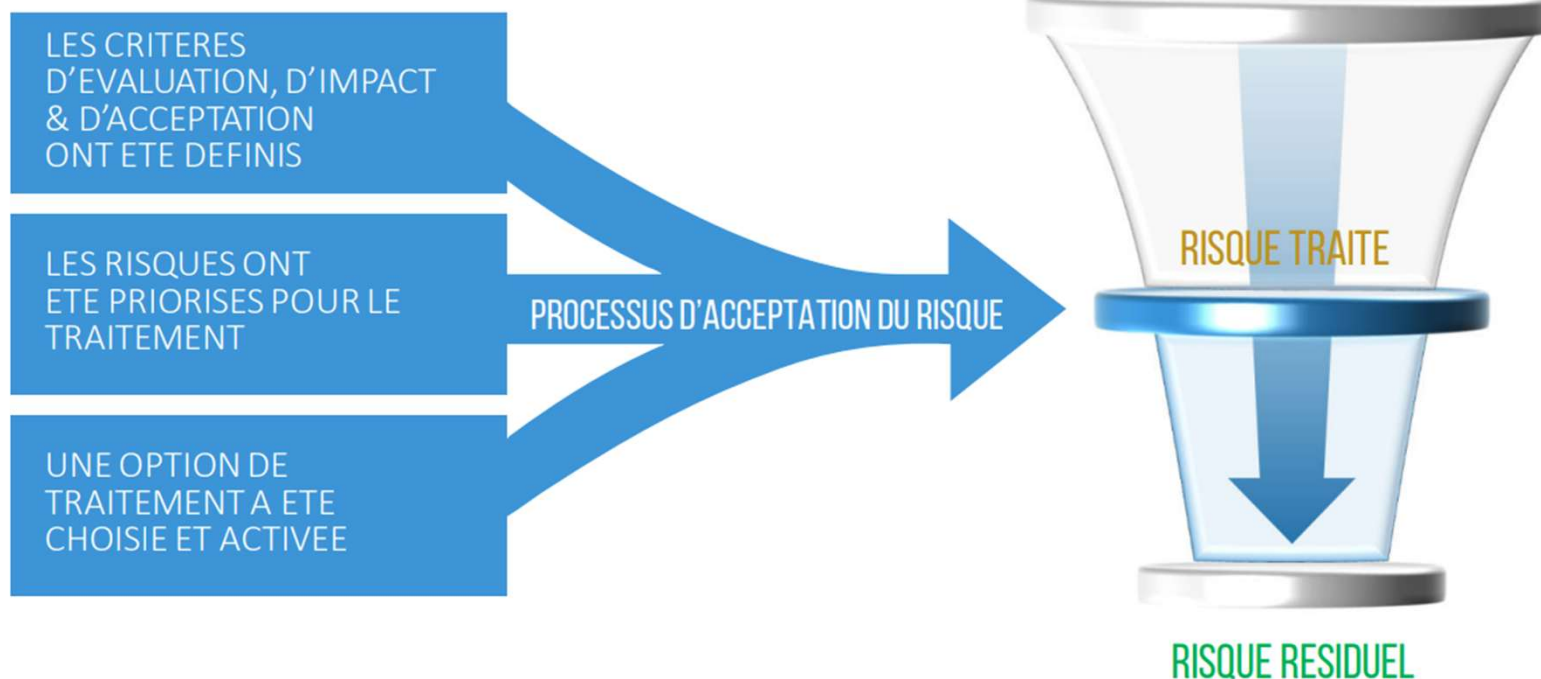
Risque tolérable seulement si le coût de réduction est extrêmement disproportionné pour atteindre le but ou les coûts excèdent l'amélioration réalisée

RISQUES RÉSIDUELS

L'organisation assurera que le risque est géré pour le garder à ce niveau ou le réduira plus si c'est pratiquement faisable

Acceptation du risque

Risque inhérent – risque traité = risque résiduel



Communication sur les risques

La communication sur le risque est une activité qui permet d'obtenir une convention sur le traitement du risque par l'échange et/ou le partage entre décideurs et parties prenantes. L'information inclut sans se limiter à l'existence, la nature, la forme, la probabilité, la sévérité, le traitement et l'acceptation des risques.

Toute organisation devrait développer un plan de communication sur les risques pour le fonctionnement normal aussi bien que pour les situations de crises L'activité de communication devrait être entreprise en continu.

Objectifs de la communication sur les risques



A qui communiquer?



Constituer un **comité**, de manière qu'un débat sur les risques, sur leur niveau de priorité et le caractère adapté de leur traitement puisse avoir lieu.

Surveillance et revue des risques

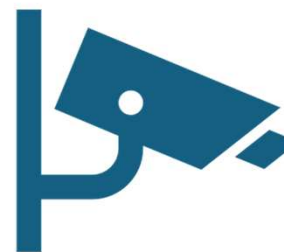
Il convient de constamment **surveiller, réexaminer et améliorer** le processus de gestion des risques en sécurité de l'information si nécessaire et de manière appropriée.

Une surveillance et une revue permanents sont nécessaires pour garantir que le contexte, les résultats de l'appréciation et du traitement des risques, ainsi que les plans de gestion, restent adaptés aux circonstances.

Surveillance et réexamen des risques



Les risques ne sont pas statiques. Les menaces, les vulnérabilités, la vraisemblance ou les conséquences peuvent changer brutalement sans aucune indication préalable.



Une surveillance constante est nécessaire pour détecter ces changements. Elle peut être assurée par des services externes qui fournissent des informations relatives à de nouvelles menaces ou vulnérabilités, comme les CIRTs, les CERTs, Les bulletins de nouvelles, les avis de sécurité, etc.

Surveillance et réexamen des risques

Pour une meilleure résilience face et aux risques et assurer l'amélioration continue



AUDIT ET CONTRÔLE INTERNE

Le but est d'aider l'organisation à accomplir ses objectifs en fournissant une approche systématique et disciplinée pour évaluer et améliorer l'efficacité des processus de gestion et de contrôle ainsi que de la gouvernance des risques.

REVUE DE DIRECTION

Le but est de réviser et d'évaluer l'efficacité du système de management et de s'assurer que tous les niveaux de management sont sensibilisés aux changements, évolutions, révisions, etc.

SUPERVISION, MESURAGE, ANALYSE ET ÉVALUATION

Le but de la supervision, du mesurage, de l'analyse et de l'évaluation est de fournir aux décideurs une compréhension de la situation concernant la performance des processus.

Surveillance, mesurage, analyse et évaluation des risques

Méthodes pour assurer l'adéquation du programme sur le long terme



■ SURVEILLANCE

Inspection ou observation continue du processus de performance ou du processus de livrables pour un objectif spécial à travers un périmètre défini (ex: selon une période de temps) et conservation de traces de ces observations.



■ ANALYSE

Ensemble de techniques permettant d'examiner les tendances de mesurage de la qualité ou de l'adéquation d'un livrable.



■ MESURAGE

Activité qui permet d'utiliser des données selon une certaine méthode pour définir objectivement un indicateur quantitatif ou qualitatif et 'capturer' ainsi une situation sans aucune référence à la signification de ses éléments constitutifs.















■ ÉVALUATION

Action de comparer un processus ou des mesures de production de processus à des critères donnés pour déterminer la performance du processus ou de la conformité d'une production de processus.

Surveillance des risques au quotidien

- 1 SIGNAL D'APPARITION D'UN RISQUE ÉLEVÉ APPARAÎT POUR PRISE EN COMPTE PLUS RAPIDE
- 2 FOURNIT DES ÉLÉMENTS SUR LES RISQUES PASSÉS POUR L'AMÉLIORATION CONTINUE
- 3 FACILITE L'ANALYSE ET LE REPORTING DES TENDANCES
- 4 MESURE FACTUELLEMENT L'APPÉTANCE ET LA TOLERANCE AU RISQUE DE L'ORGANISME
- 5 AUGMENTE LA PROBABILITÉ QUE L'ORGANISME ATTEIGNE SES OBJECTIFS STRATÉGIQUES
- 6 OFFRE UNE ASSISTANCE DANS L'OPTIMISATION DE LA GOUVERNANCE DES RISQUES

Surveillance des risques par la veille sur les vulnérabilités

	CrowdStrike	▼		ESET Threat Intelligence	▼		Recorded Future	▼
	ThreatConnect	▼		ZeroFox	▼		Flashpoint	▼
	IntSights	▼		SolarWinds	▼		Anomali	▼
	Bitdefender	▼		Cisco Talos	▼		Cisco	▼

Survol des mesures de contrôles



Contrôles ou mesures de sécurité

Les contrôles de sécurité, qui sont des mesures de protection mises en place pour atténuer les risques liés à la sécurité de l'information, jouent un rôle crucial dans la réduction de risque comme:

- prévenir les incidents;
- détecter les menaces en temps réel;
- corriger les vulnérabilités;
- dissuader les acteurs malveillants.
- Etc..

Catégories de controles

- **Les contrôles administratifs/managériaux**, qui traitent de la composante humaine de la cybersécurité à travers des politiques et des procédures .
- **Les contrôles techniques**, qui comprennent des solutions telles que les pare-feux, les systèmes de détection et de prévention des intrusions, les produits antivirus et le chiffrement
- **Les contrôles physiques/opérationnels**, qui visent à limiter l'accès physique aux actifs par des personnes non autorisées.

Exemple de contrôles administratifs



Sensibilisation à la cybersécurité



Vérification des antécédents



Politiques de mot de passe



Politique de contrôle d'accès



Gestion des comptes



Séparations des tâches et des fonctions



Etc..

Exemple de contrôles techniques



PARE-FEU



SYSTÈME EDR



CHIFFREMENT



SYSTÈME
IPS/IDS



SEGMENTATION
DU RÉSEAU



GESTION DE
RUSTINES



SAUVEGARDE

Exemple de contrôles physiques/opérationnels



Serrures et clés



Détection et prévention
d'incendie



Vidéosurveillance
(CCTV)



Systèmes biométriques
(cartes de contrôle
d'accès, scan de l'iris,
vérification des
empreintes digitales)



Générateurs de
secours



Systèmes d'alarme



Etc...

Les types de contrôles de sécurité (leur fonction)

Ces quatre fonctions de contrôles
sont de types:

Préventifs

Correctifs

Détectifs

Dissuasifs

Contrôles préventifs

Les contrôles préventifs sont conçus pour empêcher les incidents de sécurité avant qu'ils ne se produisent. Ils visent à réduire la surface d'attaque et à renforcer les défenses pour décourager les acteurs malveillants.

- Pare-feu pour filtrer le trafic malveillant,
- Politiques de mot de passe pour prévenir les compromissions de comptes,
- Principe du moindre privilège pour limiter l'accès aux données
- Outils d'évaluation des vulnérabilités et de tests d'intrusion (VAPT).

Contrôles détectifs

Les contrôles de détection déclenchent des alertes pour informer les administrateurs système ou les propriétaires de contrôles d'une tentative de violation ou d'intrusion. Donc leur rôle est de surveiller les anomalies de trafic afin d'identifier et isoler les menaces connues.

- Systèmes de gestion des informations et des événements de sécurité (SIEM)
- Vidéosurveillance
- Systèmes de détection et de réponse des points de terminaison (EDR)
- Évaluations des risques

Contrôles correctifs

Les contrôles correctifs traitent les situations « juste au cas où » c'est-à dire restaurer les données perdues ou corrompues afin de minimiser les dommages et assurer la continuité des activités.

- Systèmes de réponse aux incidents
- Récupération de données
- Déploiement des correctifs
- Isolement et quarantaine
- Intelligence des menaces (threat intel)

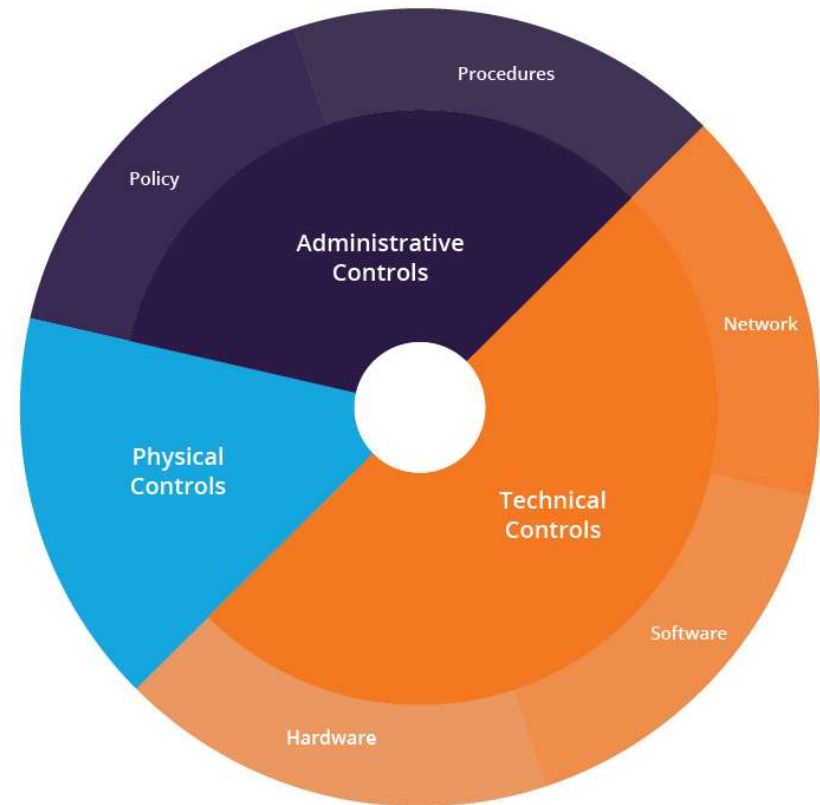
Contrôles dissuasifs

Les contrôles dissuasifs découragent la violation des politiques de sécurité et réduisent ou éliminent les motifs de comportements non autorisés, par exemple

- Les serrures de porte,
- l'éclairage,
- les caméras de vidéosurveillance,
- les suspensions,
- les amendes.

En conclusion

Ces contrôles forment une architecture de sécurité intégrée, essentielle pour prévenir, détecter, corriger et dissuader les menaces. Une stratégie de cybersécurité efficace nécessite une approche multicouche et une évaluation continue.



Questions ?

En avez-vous?



Références (1)

<https://www.knowledgehut.com/blog/security/cyber-security-plans>

<https://www.bitsight.com/glossary/cyber-security-pla>

https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf

<https://www.igniteplatform.com/blog/security/cybersecurity-procedures-controls-policies/>

<https://blog.nettitude.com/how-to-build-a-strategic-cyber-security-plan>

<https://www.apptega.com/templates>

<https://sprinto.com/blog/list-of-iso-27001-policies/>

<https://hightable.io/iso-27001-policies/>

<https://blog.netwrix.com/2023/03/03/data-lifecycle-management/>

Références (2)

- <https://corporatefinanceinstitute.com/resources/career-map/sell-side/risk-management/risk-transfer/>
- https://www.shs-conferences.org/articles/shsconf/pdf/2021/40/shsconf_glob2021_03019.pdf
- <https://flare.io/learn/resources/blog/threat-intelligence-tools/>
- <https://flare.io/learn/resources/blog/threat-intelligence-sources/>
- <https://cloudsecurityalliance.org/research/working-groups/data-security>
- [**https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/**](https://dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/)