Analyse de risque détaillé

Table des matières

Introduction

Objectif du document

Ce document détaille le processus d'analyse de risque et permet de mettre en place les plans de gestions de risques.

Objectif de l'analyse de risque

Un risque est un événement qui peut avoir un impact sur un système, il en existe deux grands types : les risques négatifs, nommés dangers et les risques positif, nommés opportunité.
Ces risques doivent donc être pris en compte dans l'organisation de l'entreprise.

L'analyse de risque est faites pour les identifier, connaître leurs impacts, et leurs chance d'occurence pour ensuite mettre en place des plans de gestion des risques.
Ainsi, l'entreprise pourra adopter un comportement adéquat face à eux.
Pour finir, une surveillance sera mis en place pour vérifier le bon déroulement des plans de gestion de risque et l'acuité de ceux-ci sur une échelle à long terme.

Chaque plan auront un coût pour les implémenter mais auront un retour sur investissement augmenté au fil du temps. L'analyse porte donc sur des solutions pour du long terme.

Contexte

L'entreprise Motuc souhaite améliorer l'efficacité de son service et réduire les dysfonctionnement (panne de courant, réseau internet hors service, ...) en mettant en œuvre un plan d'urbanisation.
L'analyse de risque est l'une des parties de l'urbanisation.

Le but est d'identifier les risques liés à l'entreprise, analyser leurs impact et fréquence pour ensuite mettre en place des plans de gestions de risques.

Identification des risques

Il existe deux types de risques : les dangers et les opportunités qui sont respectivement négatif et positif sur l'entreprise.

Pour les identifier, il faut parcourir toutes les ressources à notre disposition. Dans notre cas, nous avons le PDF expliquant le fonctionnement de l'entreprise, les plans des différentes infrastructures de l'entreprise et un rapport des dysfonctionnements observés.

Ensuite, nous pouvons les regrouper par catégorie de problème via un Risk Breakdown Structure (RBS).

Nous avons trouvé pertinent la séparation entre danger et opportunité pour augmenter la compréhension du document et mieux les traiter par la suite.

Risk breakdown structure (RBS) des dangers de Motuc

Niveau 0	Niveau 1	Niveau 2
Risques internes	Risque liés à l'infrastructure physique	Électrique (panne de courant)
		Serveur
	Risque liés à l'infrastructure réseau	Réseau et intranet
		Base de donnée
	Risque liés aux applications	Outil de gestion (ERP)
	Risque lié à un service non opérationnelle	Service caisse
		Préparation de bon de commande
		Réapprovisionnement
		Commande auprès du fournisseur
		Gestion du personnel
		Réparation
		Préparation de colis
		Installation de home-cinéma
	Risque liés au personnel de travail	Absence à un poste
		Malveillance
		Relation à l'intérieur et entre les équipes
Risques externes	Risque lié au fournisseur	Fournisseur
		Réception du stock
	Risque lié à la livraison	Livraison au magasin
	Risque liés aux concurrents	Espionnage
		Attaque au réseau (mail, DDOS, …)
	Autre	Incendie

Risk breakdown structure (RBS) des opportunités de Motuc

Niveau 0	Niveau 1	Niveau 2
Risque lié à l'entreprise	Risque lié à une fin de tâche	Réapprovisionnement anticipé
		Stockage fini
	Risque lié à une demande	Demande de réparation accrue
		Demande d'installation de home-cinéma accrue
	Risque lié à un surplus de bénéfice	Magasin très efficace
		Réduction des coûts généraux

Analyse qualitative

L'analyse qualitative cherche à exprimer les risques selon des critères :
- La capacité de détection
- L'impact : effets positif ou négatif sur le système
- Le temps de réponse ou temps de réallocation : temps nécessaire pour régler le problème ou pour allouer les ressources en excédent
- Le contrôle : la possibilité que l'on a de continuer les processus touchés par le danger ou que le problème affecte les processus (s'il est positif)

Ces critères nous ont permis d'établir ce tableau :

Analyse de risque quantitative des danger

	Capacité de détection	Impact dans le système	impact externe	Temps de réponse (en jour)	Contrôle
Panne de courant	Aucune	Arrêt de la structure	Perte de temps dans d'autre service	1 jour	faible
Panne d'un serveur	Outil de contrôle	Arrêt du service	Perte de temps dans d'autre service	1/2 journée	fort
Panne du réseau	Outil de contrôle	Pas d'internet	Perte de temps dans d'autre service	1/2 journée	moyen
Panne intranet	Outil de contrôle	Pas de communication dans l'entreprise	Perte de temps dans d'autre service	1/2 journée	moyen
Base de donnée non disponible	Outil de contrôle	Pas d'archivage ni de rapport/ bilans	-	1/2 journée	moyen
Outil de gestion (ERP)	Retour employées	Arrêt de la gestion d'un processus	Perte de temps dans d'autre service	1/2 journée	faible
Processus de préparation de colis stoppé	Message du service	Retard d'envoie des colis	-	1/2 journée	moyen
Arrêt de la réalisation bon de commande	Message du service	Retard d'envoie des colis	-	1/2 journée	moyen
Arrêt de réapprovisionnement	Outil de contrôle	Retard important d'envoie des colis	-	environ 4 jours	faible
Manque de pièce pour les réparations	Base de donnée du stock	Retard dans les réapparitions	Perte de clients	inconnu	moyen
Manque de pièce pour l'installation de home-cinéma	Base de donnée du stock	Retard d'installation d'home-cinéma	Perte de clients	inconnu	moyen

	Capacité de détection	Impact dans le système	impact externe	Temps de réponse (en jour)	Contrôle
Absence à un poste (maladie, …)	Planning	Baisse de performance du service	-	2 jours	moyen
Malveillance	Logs	Perte de données chez les concurrents	Pertes économiques	inconnu	aucun
Relation dans les équipes dégradées	Retour employées	Baisse de performance du service	-	inconnu	moyen
Perte de fournisseur	Message du fournisseur	Retard important d'envoie des colis	Pertes économiques	inconnu	aucun
Fournisseur en rupture de stock	Message du fournisseur	Retard important d'envoie des colis	Pertes économiques	inconnu	faible
Livraison au magasin avorté par la société de livraison	Logs	Retard d'envoie des colis	Perte de temps	4 jours	aucun
Epuisement volontaire de stock	Aucune	Retard important d'envoie des colis	Pertes économiques	inconnu	aucun
Attaque au réseau (mail, DDOS, …)	Outil de contrôle	Baisse de performance du réseau	Pertes économiques	1/2 journée	aucun
Incendie	Alarme incendies	Perte de matériel et de donnée	Perte économique	inconnu	moyen
Service caisse	Retour employées	Arrêt de tout le processus du magasin	Perte économique	1 jour	faible

Nous avons ensuite fait la même chose pour les opportunités :

Analyse de risque quantitative des opportunités

	Capacité de détection	Impact dans le système	impact externe	Temps de réallocation des ressources	Contrôle
Réapprovisionnement anticipé	Planning défini	-	Magasin réapprovisionné en permanence	2 jours	fort
Stockage fini	Plus de marchandise en arrivage ou à stocké	-	Stock prêt à être récupérer immédiatement	2 jours	fort
Demande de réparation accrue	Service débordée	Temps de réparation plus long	Attente client	3 semaines	faible
Demande d'installation de home-cinéma accrue	Service débordée	RDV installation plus lointain	Attente client	3 semaines	faible
Réduction des coûts généraux	Bilan coût généraux	-	Augmentation du chiffre d'affaire	6 mois	moyen
Magasin très efficace	Chiffre d'affaire supérieur à celui des autres magasins	-	Augmentation du chiffre d'affaire	6 mois	moyen

A partir de ces deux tableaux, nous avons pu convertir les champs du tableau en valeur allant de 0 à 100. Pour cette étape une concertation avec l'équipe est nécessaire pour avoir un bon résultat.
Par la suite, ces données sont utilisés pour réaliser les graphiques (figures 1, 2, 3, 4 et 5 en annexe). Ils permettent d'avoir une représentation plus visuel et de mieux identifier les points faibles à améliorer dans l'analyse de risque.

Tout les dangers avec un cumul impact et de temps de réponse (plus de 100%) ou une faible détection et un faible contrôle (moins de 100 %) devront être traités obligatoirement par la suite.

Les opportunités avec un fort impact devront être augmentés et/ou les temps de réallocation des ressources devront être diminués.

Analyse quantitative

L'analyse quantitative des risques établit une pondération.
Pour ce faire, il faut parcourir l'historique des dysfonctionnements et organiser une réunion avec les différents service. Leur point de vue et leur connaissance techniques sur le système apporteront toutes les données nécessaires pour faire l'analyse qualitative.

A partir de ces données nous pouvons créé un tableau comme suit :

Tableau d'analyse quantitative avec la provision pour risque des dangers

	Fréquence	Perte
Panne de courant	5 %	9200 €
Panne d'un serveur	10 %	2200 €
Panne du réseau	8 %	7500 €
Panne intranet	6 %	8000 €
Base de donnée non disponible	15 %	750 €
Outil de gestion (ERP)	4 %	500 €
Processus de préparation de colis stoppé	10 %	1200 €
Arrêt de la réalisation bon de commande	12 %	750 €
Arrêt de réapprovisionnement	4 %	2700 €
Manque de pièce pour les réparations	10 %	700 €
Manque de pièce pour l'installation de home-cinéma	10 %	800 €
Absence à un poste (maladie, …)	17 %	600 €
Malveillance	2 %	4400 €
Relation dans les équipes dégradées	12 %	320 €
Perte de fournisseur	3 %	3750 €
Fournisseur en rupture de stock	8 %	1400 €
Livraison au magasin avorté par la société de livraison	6 %	275 €
Epuisement volontaire de stock	2 %	8800 €
Attaque au réseau (mail, DDOS, …)	8 %	4800 €
Incendie	3 %	14000 €
Service caisse	12 %	6500 €

Tableau d’analyse quantitative avec la provision pour risque des opportunités

	Fréquence	Bénéfice
Réapprovisionnement anticipé	30 %	125 €
Stockage fini	17 %	75 €
Demande de réparation accrue	14 %	1200 €
Demande d’installation de home-cinéma accrue	9 %	3500 €
Réduction des coûts généraux	7 %	3000 €
Magasin très efficace	12 %	7000 €

A partir de ces graphiques, nous pouvons produire des graphiques représentant ces informations qui aideront à mieux visualiser l’ensemble (figures 6, 7, 8 et 9 en annexe).

Plans de gestion des risques

Introduction

Chaque plan de gestion de risque à une stratégie, un responsable de la mise en place du plan, son rôle et une description de celui-ci.

Il existe 5 stratégies pour les dangers :
- La stratégie d'intensification n'a pas de plan car le danger est définit hors de notre portée
- La stratégie d'acceptation définit que le problème n'a pas de plan pour limiter son occurence ou son impact
- Dans une stratégie d'évitement, on réduit la probabilité de subir l'impact du danger
- Une stratégie d'atténuation vise à réduire l'impact du danger lorsqu'il se produit
- Pour finir, une stratégie de transfert vise à transmettre le problème à une autre entité ou avoir une entité qui peut répondre à celui-ci

Et 5 stratégies pour les opportunités :
- La stratégie d'intensification correspond à une opportunité pour laquelle nous n'avons pas de contrôle, aucun plan ne sera fait dessus
- Dans une stratégie d'acceptation, aucun plan n'est mis en place car le rapport investissement/ bénéfice n'est pas assez important ou négatif
- La stratégie d'exploitation vise à augmenter la probabilité que l'opportunité se déclenche
- La stratégie de renforcement augmente l'impact de l'opportunité sur le système
- Et enfin la stratégie de partage permet de transférer une partie des bénéfices à une autre entité

Plans de gestion des risques liés à un incident matérielle

Panne de courant

Une panne de courant touche une grande partie de l'entreprise et immobilise plusieurs services pendant une période.
Il faut donc mettre en place plusieurs stratégies pour réduire l'occurence et l'impact du danger.

Une stratégie d'évitement sera mis en place par le service informatique. Son rôle est de contrôler que toutes les prises de la baie réseau non utilisé soient verrouillés. Cela empêchera l'agent d'entretien de créer une surtension au niveau de la plateforme.

Une stratégie d'atténuation sera mis en place par les services généraux. Leur but est d'isoler le plus possible les différents secteurs électriques de l'entreprise. De ce fait une panne d'un secteur n'influencera pas tout le bâtiment.

Enfin, une stratégie de transfert sera effectué par une société tierce s'occupant des groupes électrogènes. Son but est de les vérifié pour qu'ils soient opérationnels en cas de panne de courant.

Incendie

On aura une stratégie d'évitement mis en place par les services généraux.
Le but est de concevoir les bâtiments en respectant les normes de sécurité.
De plus les produits dangereux (réserves groupes électrogènes) doivent être loin des zones de travail des employées et les pièces ayant un fort potentiel d'incendie doivent être loin des archives et serveurs (exemple : cuisine).

Plans de gestion des risques liés à l'infrastructure réseau

Le service informatique est le responsable de tout les plans de cette partie.

Panne du réseau intranet

La panne du réseau intranet empêche toute communication dans l'entreprise. Il est donc primordiale de l'éviter.
Pour ce faire, le SI devra créer un réseau intranet secondaire qui prendra le relai en cas d'arrêt du réseau principale. La communication inter-entreprise n'aura pas ou peu d'interruption.
On applique alors une stratégie de transfert.

Panne du réseau internet

La panne du réseau internet empêche toutes connexions au réseau externe à l'entreprise. Son impact est tout aussi important que pour l'intranet.
La solution reste la même : créer un réseau internet secondaire qui prendra le relai en cas d'arrêt du réseau principale.

Panne d'un serveur

Contrairement aux deux dangers précédent, la panne d'un serveur ne touche qu'une partie du système. Malgré tout son impact reste assez important car il peut paralyser un service.

Le SI appliquera une stratégie de transfert une autre entité qui peut remplacer les pertes sur le serveur. En cas d'arrêt de certains processus, une redirection vers un service de secours dans le serveur est envisageable.

Le SI peut aussi appliquer une stratégie d'évitement en installant des outils de surveillance qui corrigeront les problèmes avant leurs apparitions.

Base de donnée (BDD) indisponible

Une stratégie d'évitement sera mis en place pour permettre la continuité du système.
Le SI créera un répliquât de la BDD principale utilisable comme solution alternative.

Plans de gestion de risques liés aux applications

Outil de gestion (ERP) hors service

Les deux seuls problèmes, relevés par le service comptabilité, qui peuvent impacter l'ERP sont la panne du réseau intranet (traité dans la partie au-dessus) et les problèmes liés aux maintenance de l'application.

Pour le résoudre, le SI devra s'assurer que les maintenances se déroulent pendant les heures creuses (pause repas, après les horaires de travail, ...). Ce sera donc une stratégie d'atténuation, car nous cherchons à réduire l'impact sur les services.

Plans de gestion de risques liés aux services

Arrêt du processus de préparation de colis

Ce risque a un impact faible et un temps de réponse court. Nous l'avons donc défini d'acceptable sur notre système. Le chef de préparation de colis appliquera une stratégie d'acceptation. Seul une avance du service sur la préparation des colis peut réduire son impact.

Arrêt de la réalisation bon de commande

Encore une fois, l'impact de ce risque est faible. Quelques mesures préventives peuvent être prise par le chef du service de réparation en vérifiant le matériel permettant le bon fonctionnement de ce processus (imprimante, postes de travail, ...).

Demande de réparation de produit ou d'installation de home-cinéma accrue

On a deux stratégies à appliquer pour cette opportunité :
- La première est une stratégie de renforcement, le service RH doit recruter plus de personnel pour éviter un débordement du service
- La deuxième est une stratégie d'exploitation, le directeur du magasin doit faire de la publicité pour amener plus de client

---

Plans de gestion de risques liés au personnel de travail

Absence à un poste

Une absence à un poste est souvent temporaire. Il est dû à un événement imprévu comme un congé maladie, un accident, ...
Il existe plusieurs plans de gestion de ce risque en fonction de l'importance du poste inactif.

Si les ressources humaines définissent que le poste n'influe pas sur l'efficacité du service, alors, une stratégie d'acceptation sera appliqué. Une petite réorganisation du planning du service peut-être envisagé.

Si un responsable est vacant, on peut appliquer un plan en fonction de son importance :
- Si le service peut continuer à fonctionner sans lui, alors on applique une stratégie d'évitement. Le manager doit prévoir un planning de la semaine comportant les instructions des employés
- Si le responsable a aussi un rôle de contrôle (comme un chef de rayon), alors les ressources humaines devront former un assistant capable de prendre la main suffisamment pour assurer la continuité du service. Ce sera alors une stratégie de transfert.

Plans de gestion de risques liés aux rupture de stocks

Manque de pièce pour la réparation de produits ou l'installation de home-cinéma

Le chef du stock doit éviter ce risque. Pour cela il doit toujours prévoir un stock minimal qui lui permet de continuer le fonctionnement du système même en cas de pénurie.

Arrêt de réapprovisionnement

L'arrêt de réapprovisionnement peut être dû à différents facteurs comme un service débordé, des livraisons avortés, ...
Une stratégie d'évitement peut être appliqué par le chef du stock en évitant d'être à court d'un produit. De ce fait, même en temps de pénurie, le réapprovisionnement des magasins et de la plateforme commercial pourra continuer.

Réapprovisionnement anticipé et stockage fini

Une fois l'anticipation du réapprovisionnement effectué sur une période assez large. Ce surplus de main-d'oeuvre à l'arrêt peut être redirigé par le chef du service pour réorganiser le stock et optimiser le déstockage pour le service préparation. On applique une stratégie de partage.

Plans de gestion de risques liés aux fournisseurs

Perte d'un fournisseur ou fournisseur en rupture de stock

La dépendance à un fournisseur pour un ou certain type de pièces doit être éviter à tous pris, pour cela il faut que le service achat diversifie leurs nombres.
Dans le cas d'un épuisement volontaire de stock par un concurrent, le plan de gestion contre les attaques informatiques et la malveillance permettent de répondre à ce problème.

Plans de gestion de risques liés aux livraison

Livraisons avortés

Nous n'avons pas de la main dessus. Vu que l'impact n'est pas très important, nous ne nous préoccupons pas de ce problème car tout plans seraient trop coûteux.

Plans de gestion de risques liés aux concurrents et attaques extérieures

Attaque informatiques et malveillance

Les attaques informatiques ont un impact très important : blocage du réseau, vol de données, ...
Ils faut impérativement les éviter et diminuer leurs impacts.

Pour cela le service informatique appliquera deux stratégies :
- La première s'applique avant que l'attaque ne parvienne dans le réseau. Pour cela il faut augmenter le niveau de sécurité du système, mettre à jour l'équipement et de le renouveler pour toujours garder un haut niveau de protection face aux attaques. Le personnel doit être sensibilisé aux attaques informatiques et bonne conduite (exemple : ne pas laisser de clé USB contenant des informations sur l'entreprise sans surveillance) pour réduire encore plus l'occurence du risque
- La deuxième est une stratégie d'atténuation avec pour but de mettre l'infection en quarantaine. Il ne faut pas quelle s'infiltre dans tout le système. Il faut aussi que le responsable adéquat soit avertis du problème.

Plans de gestion de risques liés aux chiffre d'affaire

Baisse des coût généraux et augmentation du chiffre d'affaire

Lorsque un service à un surplus de chiffre d'affaire, il faut le rediriger vers d'autre projet, ou alors le réinvestir dans le service pour augmenter sa qualité. On adopte alors une stratégie de partage.

Pour le cas du magasin, une stratégie d'exploitation peut-être mis en place par le biais de la publicité pour faire venir plus de client.

Surveillance

But de la surveillance

La surveillance ici, n'a pas de rapport avec la surveillance des risques (partie détaillé dans le PRA et PCA) mais de pouvoir vérifier la précision de l'analyse de risque et de la faire évoluer de temps. En effet, des risques peuvent, entre-temps, augmenter au niveau de leur pondération ou d'autre caractéristiques, il faut donc à nouveau les inclure ces nouveaux paramètres. Aussi certains risques peuvent apparaître et il faudra eux aussi les traiter.

Déroulement de la surveillance

Lors de l'implémentation des plans, il sera impératif de maintenir un historique de leur implémentation. Le but est de faciliter l'implémentation de ceux-ci dans le futur.

Au fur et à mesure du temps, certains peuvent changer (impact, pondération, ...) ou d'autres apparaissent. C'est pourquoi il faudra refaire des analyses de risque pour prendre les nouveaux paramètres en considération.

Pour ce faire, il faudra collecter les informations composant le risque pour créer de nouveaux rapport et bilan.

Pour avoir une vision de ce qu'il faut faire sur cette partie, nous avons créer un tableau composé du métrique observé, du moyen de collecte des informations et des documents en sortie pour les dangers et les opportunités.

Représentation des documents à procurer via la surveillance

	Métrique	**Moyen de collecte des informations**	**Document**
Panne d'un serveur	Taux de disponibilité d'un serveur	Alerte et rapport envoyé depuis l'infrastructure (routeur, switchs, serveurs, …)	Rapport sur l'infrastructure réseau
Panne du réseau	Taux de disponibilité du réseau		
Panne intranet	Taux de disponibilité du réseau intranet		
Base de donnée non disponible	Taux de disponibilité		
Attaque au réseau (mail, DDOS, …)	Nombre d'attaque		
Processus de préparation de colis stoppé	Période hors-service	Rapport du service post incident	Rapport du taux d'activité des services
Arrêt de la réalisation bon de commande	Période hors-service		

	Métrique	Moyen de collecte des informations	Document
Arrêt de réapprovisionnement	Période hors-service		
Service caisse	Période hors-service		
Manque de pièce pour les réparations	Stock des fournitures	Rapport du service de comptabilité du stock	Rapport du management du stock
Manque de pièce pour l'installation de home-cinéma	Stock des fournitures		
Malveillance	Nombre de fourniture en doublon sans erreur de commande	Rapport d'enquête internes	
Perte de fournisseur	Nombre de fournisseur pour une catégorie de produit	Catalogue des fournisseurs	Bilan des échanges avec les fournisseurs
Fournisseur en rupture de stock	Stock fournisseur	Stock des fournisseurs	
Epuisement volontaire de stock	Quantité de fourniture accaparé par un concurrent		Bilan des attaques concurencielles
Outil de gestion (ERP)	Période hors-service	Rapport de panne de l'outil fait par le SI	Rapport du taux de disponibilité des outils informatiques
Panne de courant	Nombre de coupure de courant	Bilan des pertes financières de la coupure de coupure	Bilan de la gestion des crises
Incendie	Nombre d'incendies	Bilan des pertes financières de l'incendie	
Livraison au magasin avorté par la société de livraison	Nombre de commandes avortés	Rapport entre le planning théorique et réel	Rapport des livraisons effectuées/ avortés
Absence à un poste (maladie, …)	Nombre d'absences de l'entreprise	Planning des employés	Rapport de l'efficacité des équipes
Relation dans les équipes dégradées	Satisfaction employées	Enquête de satisfaction	
Réapprovisionnement anticipé	Temps libre du sevice	Planning du service réapprovisionnement	Rapport d'efficacité des services
Stockage fini	Temps libre du sevice	Planning du service de stockage et réception	
Demande de réparation accrue	Nombre de réparation	Base de donnée du service réparation	
Demande d'installation de home-cinéma accrue	Nombre d'installation	Archive des installations	
Augmentation de la masse salariale	Nombre d'employés	Bilan de recrutement RH	
Réduction des coûts généraux	coût des nouvelles infrastructures	Rapports des coûts généraux	
Magasin très efficace	Chiffre d'affaire du magasin	Rapport du chiffre d'affaire des magasins	

Bilan

L’analyse de risque a permis d'identifier les risques et de pouvoir proposer des plans pour les gérer. Maintenant, il est possible d’établir un budget à allouer à chacun d’entre eux et d’avoir une visibilité sur l’avenir.

Les documents de la partie surveillance ne sont en rien définitif. Ils peuvent varier en fonction de votre point de vue.
Ils rejoindront bien évidemment beaucoup de documents de la partie PRA et PCA qui est la méthodologie d’implémentation de l’analyse des risques.

Tout le processus d’analyse de risque a été décris à travers ce document pour vous permettra de refaire l’analyse lors de modification ou ajout de risques. Vous serez amené à modifier ce document lors de mise à jour de l’analyse.

Annexes

Figure 1 - Cumul de l'impact et du temps de réponse des dangers

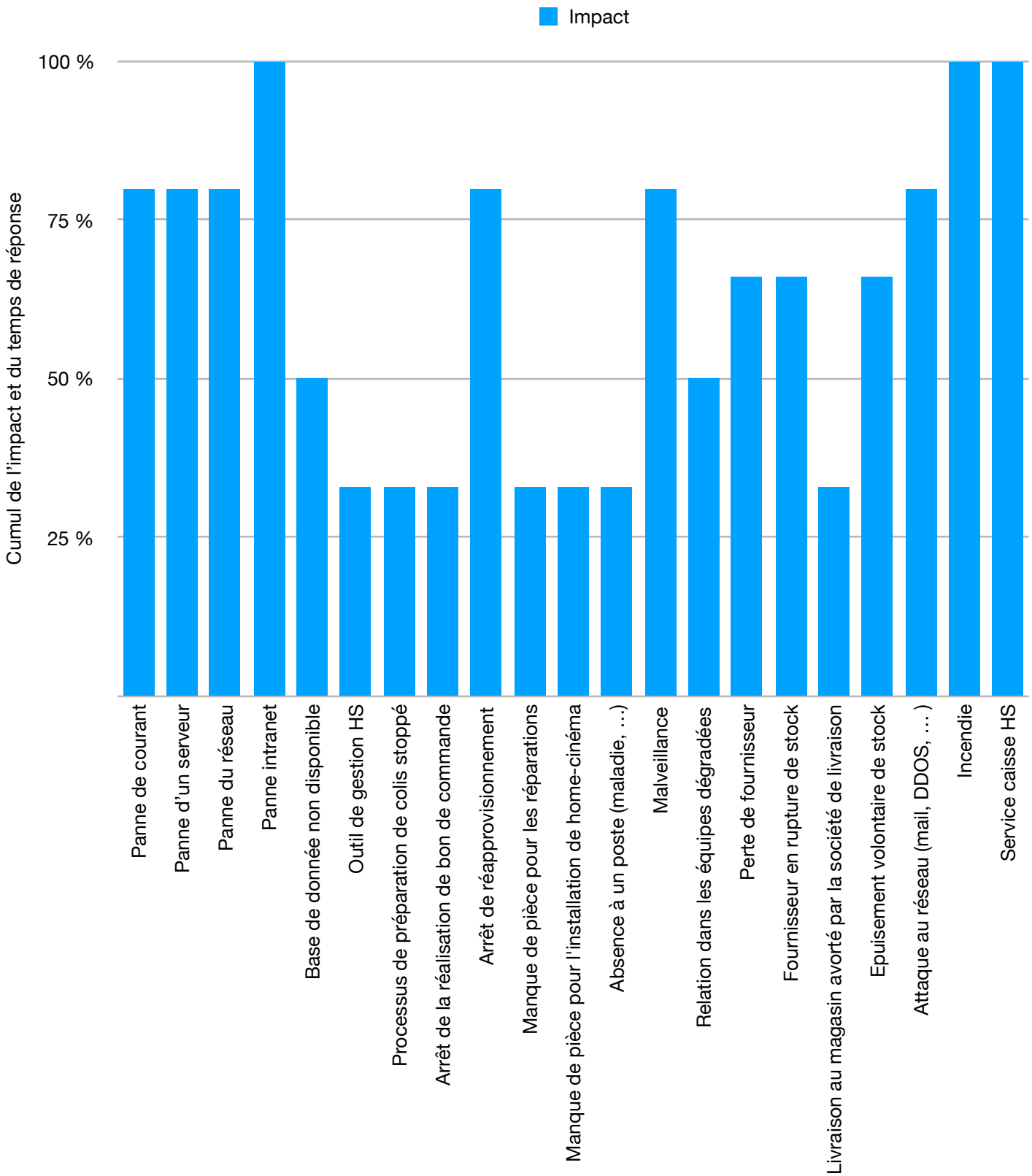

Figure 2 - Temps de réponse face au dangers en jours

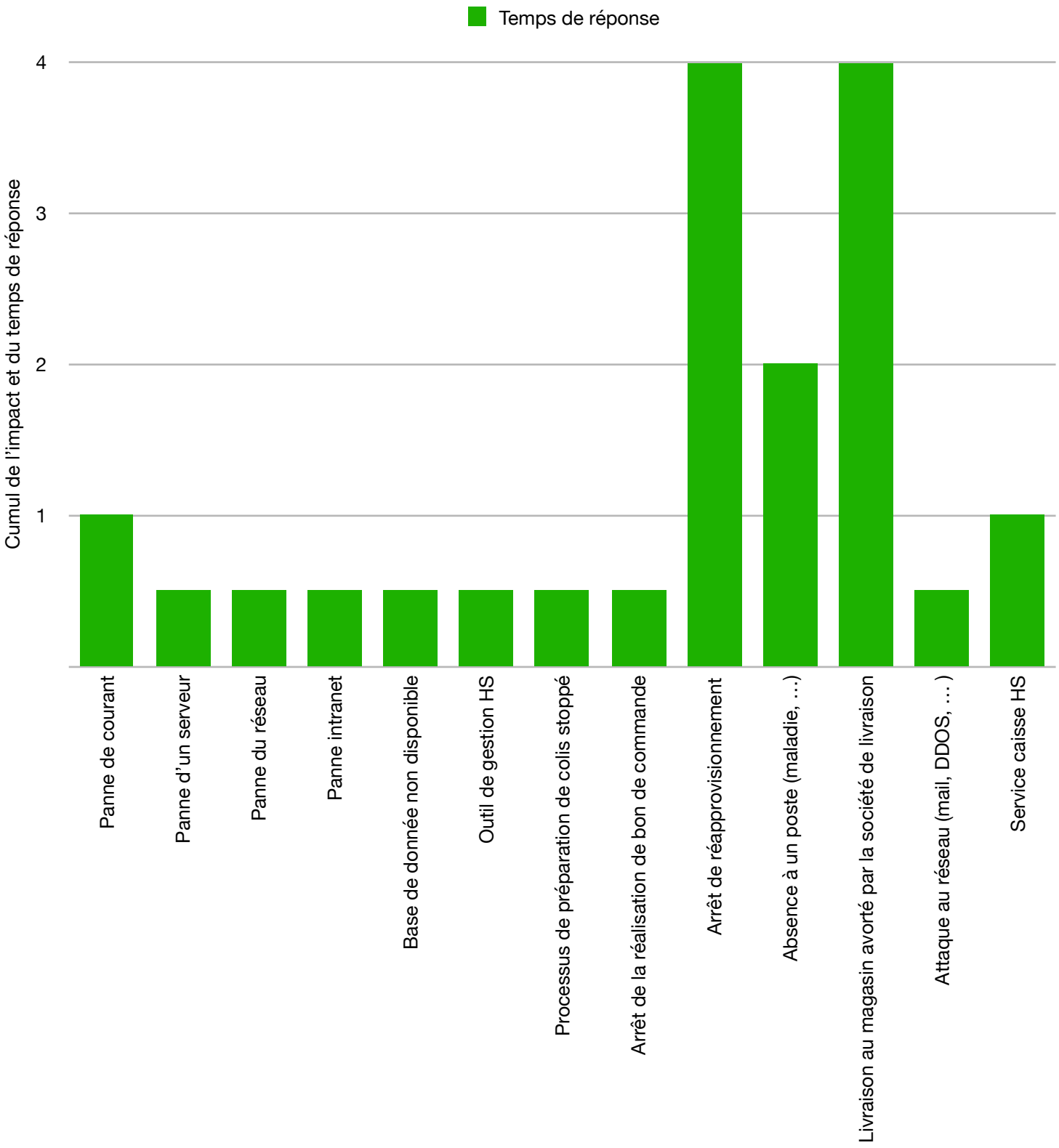

Figure 3 - Cumul de la capacité de détection et du contrôle des dangers

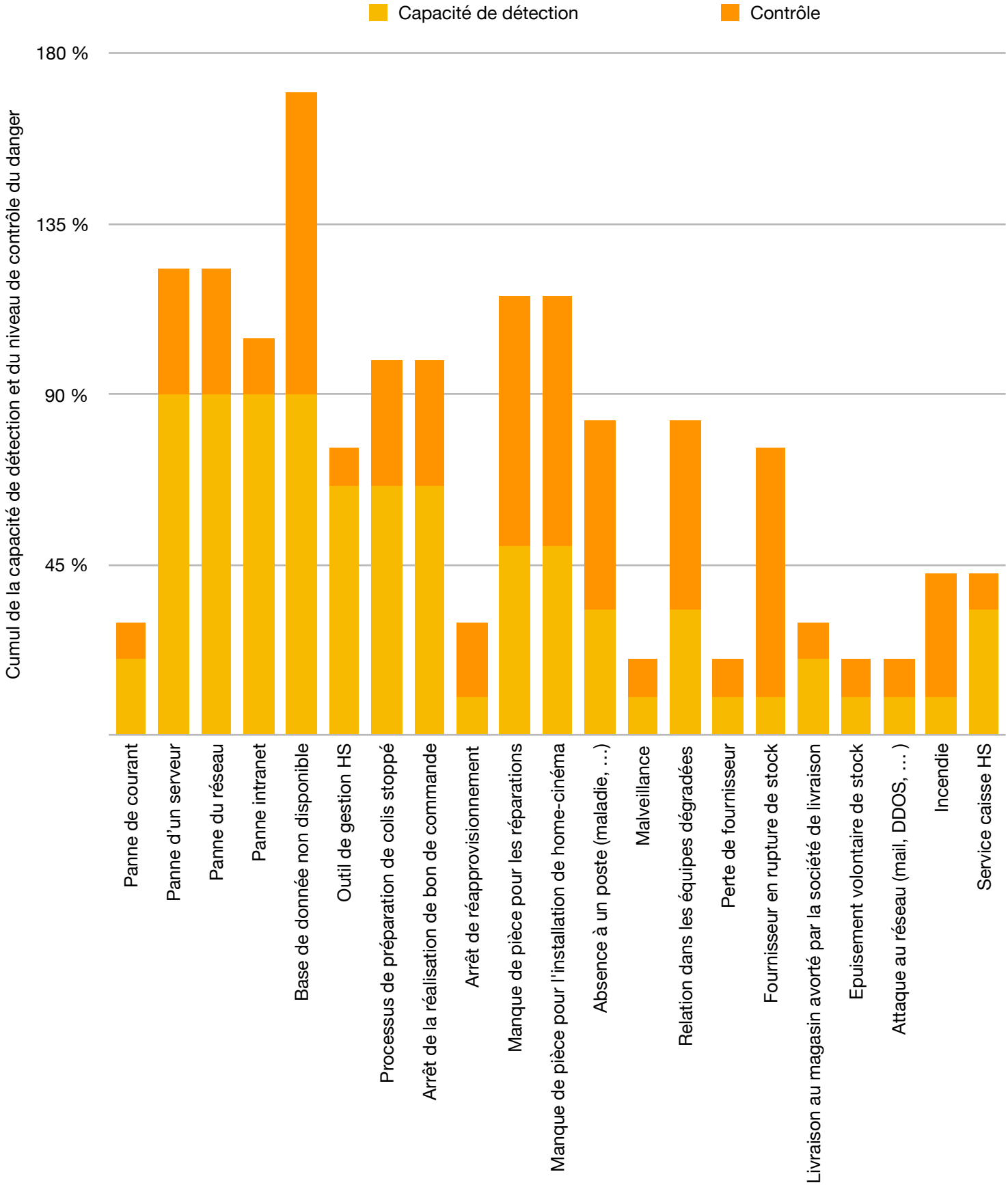

Figure 4 - Cumul de la capacité de détection, du contrôle et de l'impact des opportunités

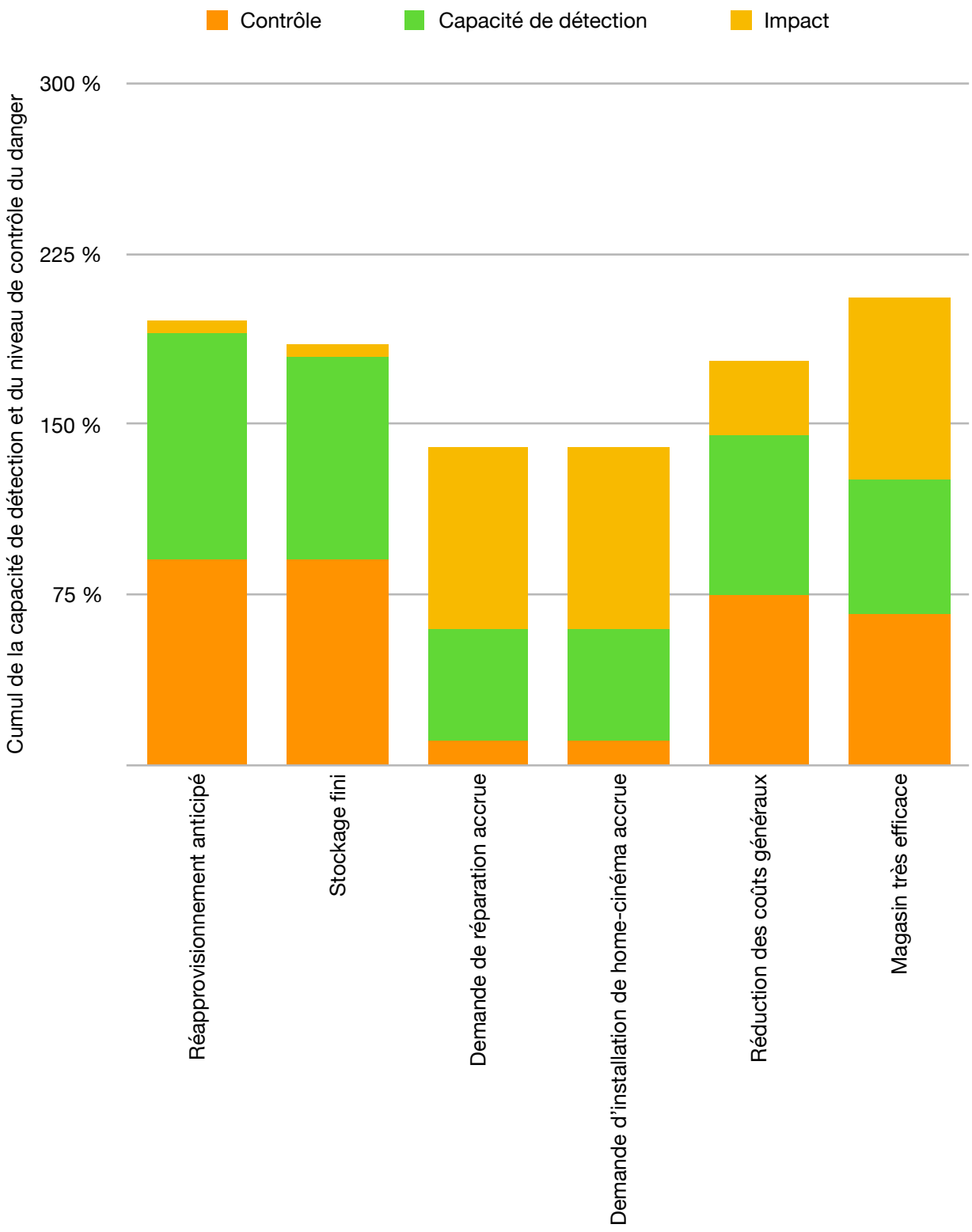

Figure 5 - Temps de réallocation des ressources des opportunités en semaine

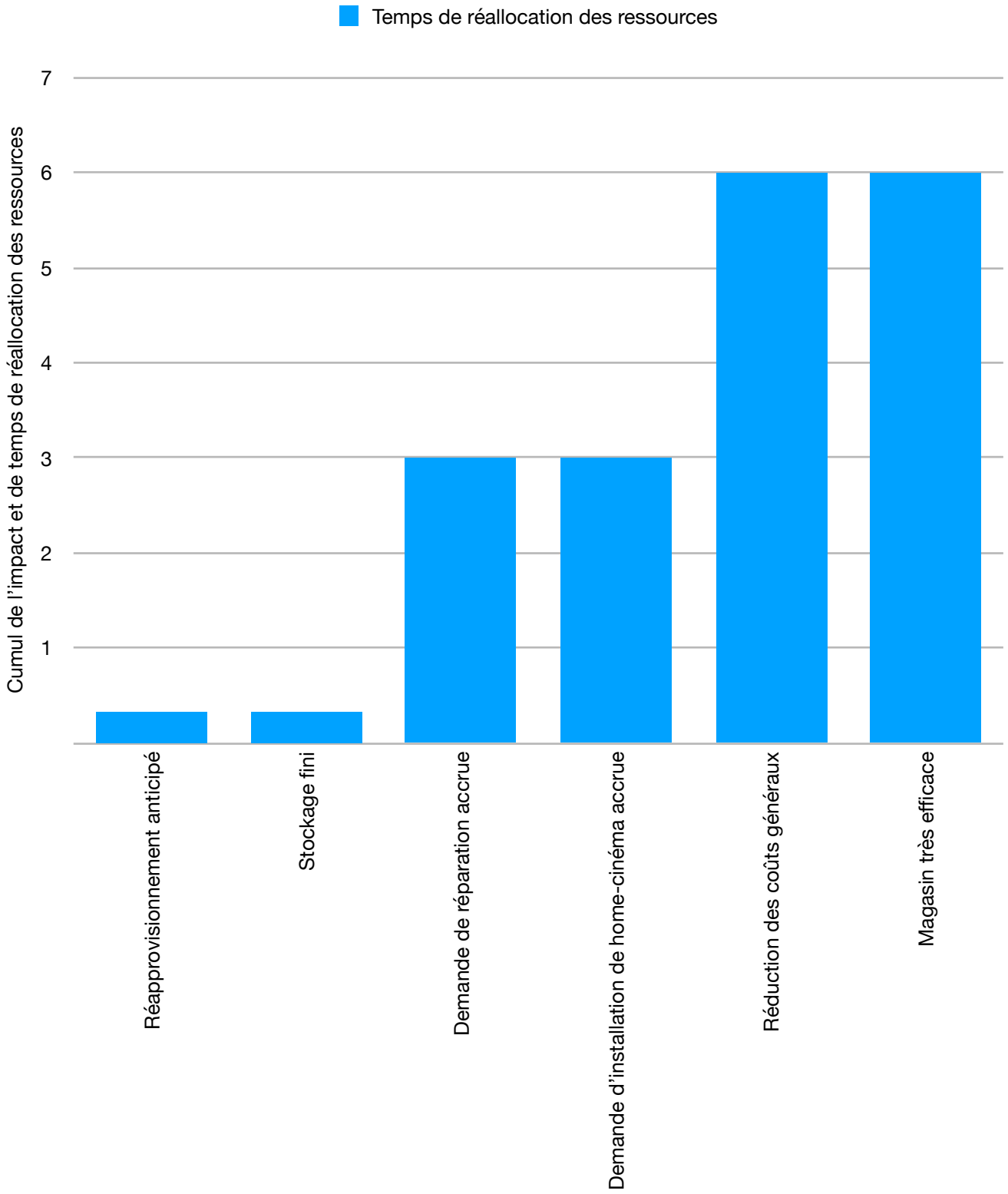

Figure 6 - Graphique de la fréquence des dangers

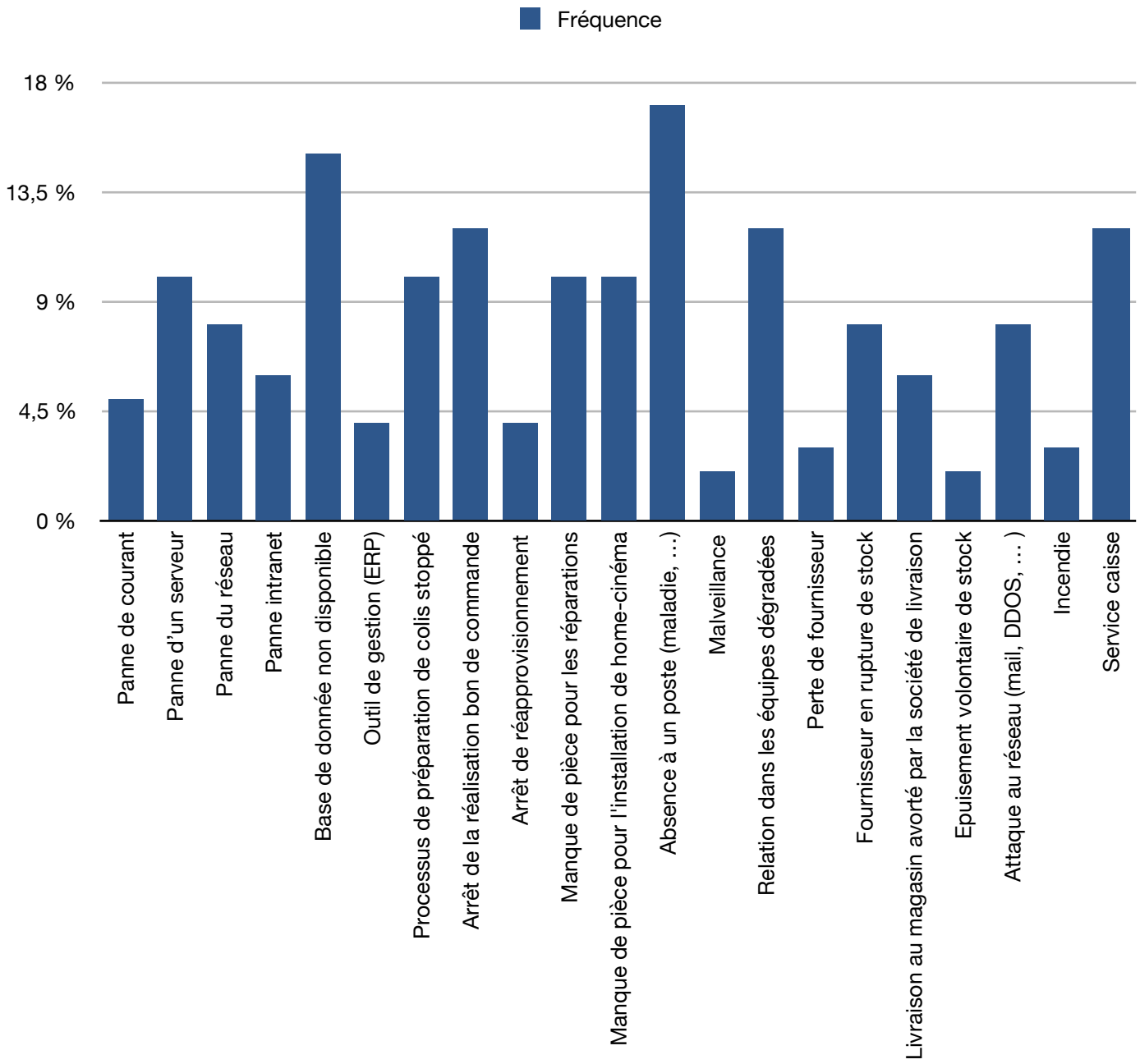

Figure 7 - Graphique du coût de chaque dangers

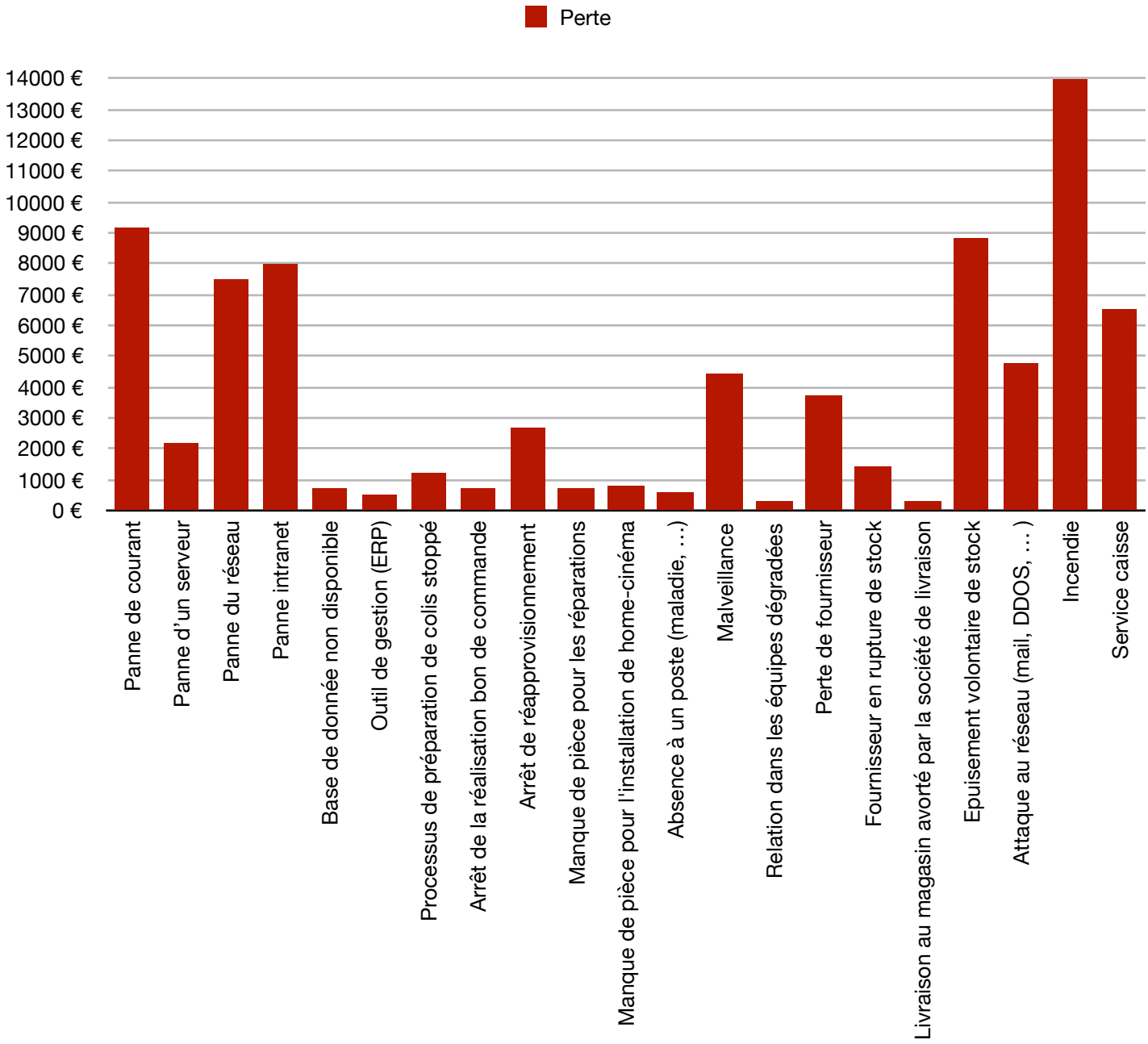

Figure 8 - Graphique de la fréquence des opportunités

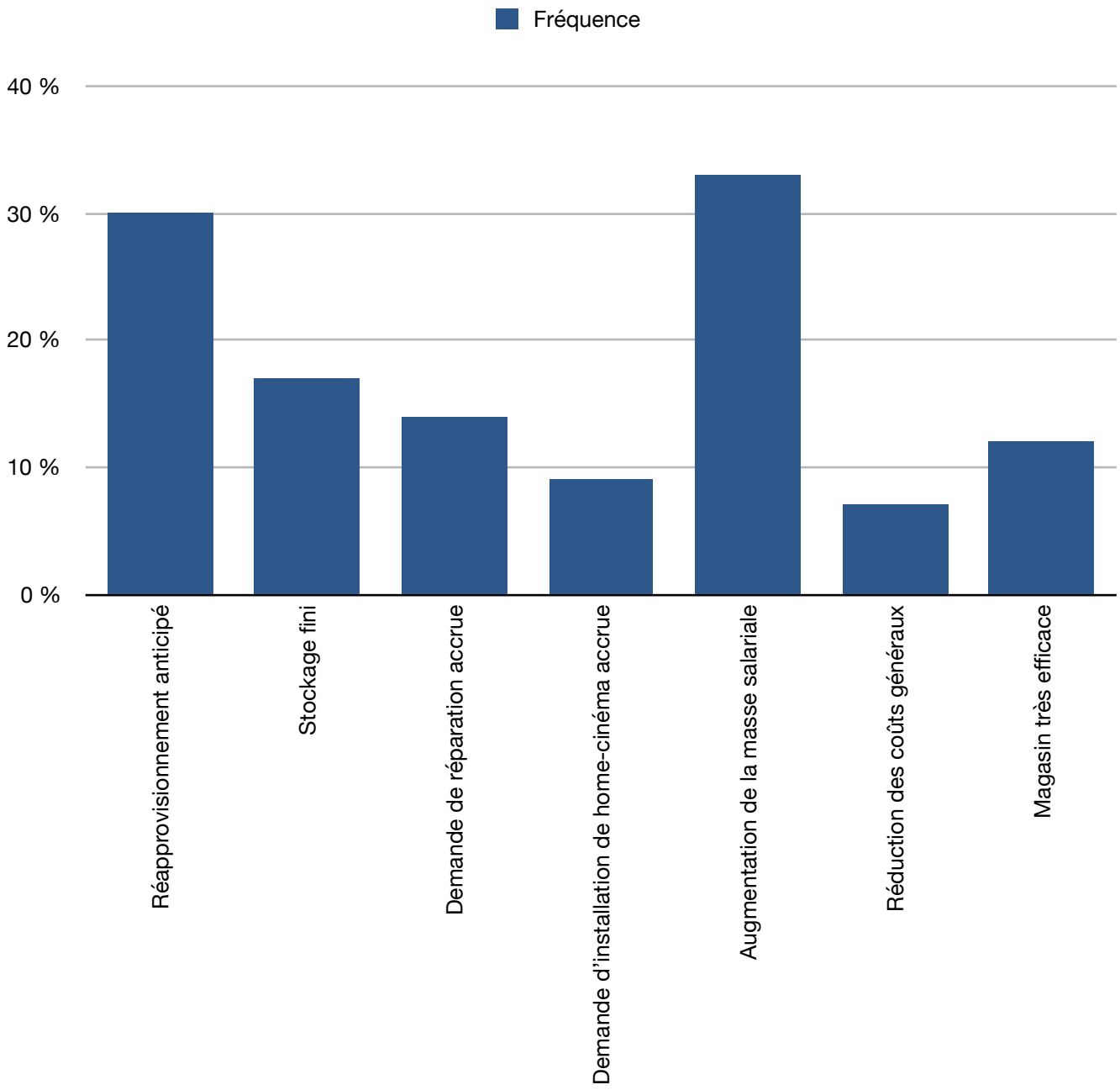

Figure 9 - Graphique du bénéfice de chaque opportunité