Bases d'architecture informatique

Eric Deblon
EFit-partners, 2020

Table des matières

Introduction

Le monde informatique foisonne de normes les plus diverses. Il en va ainsi des normes de sécurité, par exemple. Parce qu'il s'agit d'un domaine qui est au sommet des préoccupations actuelles des entreprises et qu'en conséquence elle représente un marché juteux, il existe pléthore de normes, de « *best practices* » ou de « *frameworks* » qui abordent tous plus ou moins la sécurité. À l'opposé, les objectifs de disponibilité ou de performance, pourtant tout aussi critiques en terme de risque, sont orphelins.

Face à cette prolifération côtoyant l'absence, il faut bien admettre que, parfois, on perd le fil du bon sens... De fait, une fois ces documents lus, la question qui revient invariablement est « En pratique, que doit-on faire ? ».

Le présent essai tente une approche systématique de l'architecture informatique, partant du *Service Level Agreement* (SLA) qui va fixer les objectifs de disponibilité, sécurité et performance. Le but est de clarifier les concepts et proposer l'une ou l'autre définition quand elles manquent ou si celles existant présentent des lacunes.

Il ne s'agit pour l'instant que d'un premier pas couvrant

essentiellement les concepts généraux et la disponibilité. Les prochaines versions seront étendues aux objectifs de sécurité et performance dans un premier temps et, dans un second temps, aux différentes architectures techniques permettant de répondre à chacun des trois objectifs.

Cet écrit est le fruit de l'expérience d'EFit-partners, des leçons tirées de nos essais, succès ou échecs. Il n'a finalement d'autres ambitions que d'être un guide de survie à destination des managers, gestionnaires de projets et autres malheureuses personnes qui ont l'infortune de devoir entrer en contact avec une équipe d'informaticiens.

Enfin, comme rien n'est jamais complet, toute suggestion est la bienvenue et peut être envoyée à *eric.deblon@efit-partners.com*.

Première partie

Risque et informatique

Chapitre 1

Risque

1.1 Un peu d'histoire

Le 21 novembre 1916, le navire « Britannic » coule en mer Égée au large de l'île de Kéa. Troisième et dernier exemplaire de la classe « Olympic », lui et ses deux sister-ships sont pourtant conçus pour être les paquebots les plus sûrs de leur temps, selon les dires de leur commanditaire, la White Star Line. La presse de l'époque les qualifie d' « insubmersibles ».

Le « Britannic » a coulé bien qu'il avait intégré lors de sa construction de nombreuses modifications tirées de l'expérience du naufrage, quatre ans plus tôt, dans la nuit du 14 au 15 avril 1912, du deuxième des navires de cette même classe, le « Titanic ».

Outre l'évidente cause naturelle qu'est l'iceberg, les commissions d'enquête américaine et britannique retiennent essentiellement les erreurs humaines conséquentes à une mauvaise

évaluation du risque telles la vitesse du vaisseau, la mise en œuvre inappropriée de la détection des icebergs et la désorganisation lors de l'évacuation. Les fautes de conception, que sont la taille du safran et la fragilité des rivets, ont été mise en lumière par la suite. Le rapport de la commission britannique se conclu par une série de vingt-quatre recommandations sensées prévenir ce genre de catastrophe.

Un siècle plus tard, lorsqu'on demande de citer des évènements qui représentent un risque tel pour la disponibilité d'une infrastructure informatique qu'ils peuvent être qualifiés de désastre, ce sont des catastrophes naturelles ou des attentats spectaculaires qui sont le plus souvent cités. Pourtant les drames des navires de la White Star Lines sont bien plus instructifs que les évènements destructeurs cités car ils cumulent cause naturelle, fautes de conception et erreurs de gestion.

Il est vrai qu'évoquer les éléments naturels déchainés ou la folie destructrice de l'homme comme raison d'une indisponibilité permet de s'exonérer d'une partie de ses responsabilités, voire même s'attirer une certaine empathie au titre d'un sentiment de victimisation vis-à-vis d'un élément extérieur.

On ne peut qu'être surpris par l'écart évident entre l'insubmersibilité annoncée des trois navires et le fait que deux ont fini par sombrer, victimes d'accidents auxquels ils étaient sensés résister, un iceberg pour l'un et probablement une mine pour l'autre.

Vers 1513, Nicolas Machiavel exprimait déjà ce paradoxe : « Il y a si loin de la manière dont on vit à celle dont on devrait vivre, que celui qui tient pour réel et pour vrai ce qui devrait l'être sans doute, mais qui malheureusement ne l'est pas, court

à une ruine inévitable ».[1]

Pourtant, aujourd'hui, les infrastructures informatiques présentent très souvent le même genre d'écart entre les objectifs affichés et la réalité. C'est en ce sens que l'application de la gestion du risque aux infrastructures informatiques nous a semblé pertinent.

1.2 Définition

Comme souvent, il existe pléthore de définitions pour un unique mot et, pour peu qu'il soit à la mode, chaque nouvelle méthodologie, norme ou référentiel ajoute la sienne. Il en va ainsi pour le mot « risque ». Actuellement, deux semblent vouloir s'imposer, issues des méthodologies ISO 31000 et COSO.

ISO 31000, une des dernières normes en date, « fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque »[2]. Le risque y est défini comme l'effet de l'incertitude sur l'atteinte des objectifs[3].

COSO est un référentiel de gestion du risque défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*. Sa définition du risque est « la possibilité qu'un évènement survienne et nuise à l'atteinte d'objectifs »[4].

Le but ici n'est pas de décrire les différentes méthodologies, normes ou référentiels et encore moins d'en faire une étude

[1] Niccolò Machiavelli, Le Prince, chapitre XV « Ce qui fait louer ou blamer les hommes, et surtout les princes. »

[2] https ://www.iso.org/fr/iso-31000-risk-management.html

[3] In [4], p.1

[4] In [9], p.16

comparée. De nombreux ouvrages ou sites internet s'en sont chargés et l'objectif n'est pas d'en écrire un de plus. Il nous a donc fallu faire un choix et ce choix s'est porté sur COSO2 qui est à la fois un des plus populaires et plus cohérent qu'ISO 31000.

L'approche proposée par ISO 31000 est globalement réconciliable avec celle de COSO2 mais elle n'apporte finalement rien de vraiment déterminant par rapport à cette dernière.

De plus, il faut noter une incohérence certaine au sein même des différentes normes ISO. Par exemple, parmi les normes ISO 27000 et associées, relatives à la sécurité de l'information, il existe ISO 27005 dont le titre est « Norme de gestion de risques liés à la sécurité de l'information ». En y regardant de plus près, elle est à ce point différente de ISO 31000 que même la définition du risque y est différente. Entre ISO 27005 et ISO 31000, laquelle choisir ?

C'est donc COSO2 qui servira de référence en matière de gestion du risque tout au long de cet essais. Nous nous contenterons d'en esquisser les contours et de détailler ce qui sera utile pour la suite à commencer par sa définition du risque que nous adopterons[5] :

> **Un risque est la possibilité qu'un évènement survienne et nuise à l'atteinte d'objectifs.**

Quatre mots ressortent de cette définition :

- possibilité
- évènement

[5] In [9], p.16

- nuire
- objectif

1.3 En détail

1.3.1 Possibilité

La possibilité doit être entendue dans le sens d'éventualité, du caractère de ce qui peut se réaliser[6].

La quantification de cette possibilité amène aux probabilités, COSO parle alors de **probabilité d'occurrence** ou probabilité de survenance d'un évènement.

1.3.2 Évènement

Un évènement est ce qui arrive et qui a quelque importance, dans ce cas, pour l'atteinte des objectifs[7].

Dans COSO, l'évènement est souvent appelé « facteur de risque ».

Dans la cadre de la gestion du risque, on a souvent tendance à confondre évènement et risque. Un exemple pour illustrer simplement la différence...

Un propriétaire foncier voit sa forêt brûler.

L'évènement potentiel qu'est l'incendie n'est un facteur de risque que s'il nuit à l'objectif de production de bois d'œuvre. Le risque sous-jacent est la perte monétaire due à

[6] In [2], possibilité
[7] In [2], évènement

1.3.3 Nuire

Nuire signifie « constituer un danger, causer du tort »[8].

Donc, parlant de risque, COSO ne considère que les évènements qui constituent un danger, qui pourraient causer du tort à l'atteinte des objectifs. On parle souvent d'affecter défavorablement ou négativement l'atteinte des objectifs. C'est ce côté défavorable, négatif qui induit le risque et sa quantification est l'**impact** de l'évènement sur l'atteinte des objectifs.

Par opposition, une opportunité est définie comme une possibilité qu'un événement survienne et contribue à l'atteinte d'objectifs.

1.3.4 Objectif

Un objectif est un but que l'on cherche à atteindre.

Aussi bien COSO qu'ISO 31000 définissent le risque par rapport à l'objectif poursuivi.

En pratique, cela implique qu'il n'y a pas de risque sans objectif. Hors le besoin de prendre sur soi tous les malheurs de l'humanité, il est des évènements qui n'entrent pas en ligne de compte parce que ne s'inscrivant pas dans une recherche d'atteinte d'objectif.

[8] In [2], nuire