**Risk Assesment Form** (very basic and simplified)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk** | **Who & what are in risk** | **Possible consequence(s)** | **Probability / Impact** | **Mitigation** | **Responsible for mitigation** |
| Electricity failure in datacenter | Data stored in the datacenter but not in the backup | Partial/total loss of data | Probability: D  Impact: 2  **Medium** | Copy data to backup regularly to minimize loss | IT team |
| DDOS of the online store | Client, sales | Client can’t make any purchase | Probability: C  Impact: 3  **Medium** | Install a firewall to limitate bot usage on the website | IT and Security team |
| Malware downloaded on a local computer | Workers, their work, data stored in the computer, data they have access to | Work documents can be compromised (ransomware)  Steal of private information | Probability: B  Impact: 2  **High** | Do regular campaign of prevention, prevent automatic download on computer and systematically scan downloaded files. Can also limit usage of internet on computer that does not need it | Everyone |
| A server that stops working unexpectedly (overheat, …) | Client, sales, other server (traffic redirected) | Loss of sales (slower service), damage on other servers, | Probability: C  Impact: 4 (does not stop the service totally)  **Low** | Doing maintenance on server regularly  Monitor server status at all time  Have several servers that can take the place of the other | IT Team |
| Flooding | Server, datacenter, all services | All services are unavailable, all data are lost | Probability: E  Impact: 1  Medium | Server room should not be on the first floor, datacenter and databackup should not be in the same room, and not in the same building if possible | Person choosing room repartition |

Probability :  
E : improbable → could happen, but would be surprising (every 30years)

D : Remote → Happened rarely, every 5years

C : Occasional → Could happen once in one or 2 years

B : Probable → Can happen several time in one year

A : Frequent → Can happen every month

Impact :

4 : Negligible → All services are still available, with maybe a slow down

3 : Marginal → Some services are not available, but overall most of services are available, some users can be impacted

2 : Critical → Majority of services are not available, but some of them (minority) are still available, can be putted back into services after fixing

1: Catastrophic → All the services are unavailable, and can not be restored

RISK - chance or probability that person/asset will be harmed or suffers damage (KISS: probability of something bad happening)

RISK = Likelihood x impact

THREAT - situation or activity that can cause harm

