**OCTAVE: - (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**

**Developed by: - Carnegie Mellon University's Software Engineering Institute.**

**OCTAVE aligns with industry best practices and standards such as ISO-27001 and NIST cybersecurity framework.**

**Allegro has shifted OCTAVE from a technology asset centric to information asset centric.**

**Step 1 – Establish Risk Measurement Criteria**

**Step 2 – Develop an Information Asset Profile**

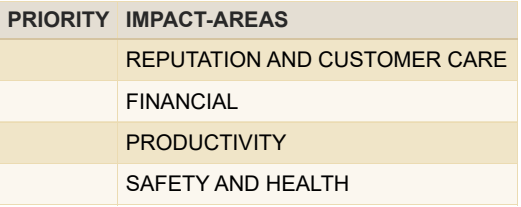
**Step 3 – Identify Information Asset Containers**

**Step 4 – Risk Calculation**

**Step 5 – Risk Mitigation**

**STEP-1) We have defined major impact areas and prompt the user with questions for every impact area: -**

* 1. Reputation and Customer Confidence
  2. Financial
  3. Productivity
  4. Safety and Health
  5. Fines and Legal Penalties
  6. We can also add user defined, if necessary, by the user.



**STEP-2) Developing asset profile: - (Add-On)**

**STEP 2.1 -** We then make a profile of the asset to get a brief knowledge and understanding of the asset.

**STEP 2.2 –** We then ask the user to categorize the impact areas in decreasing order of their risk value **(PRIORITY ORDER)**.

**STEP-3) Identify Information Asset Containers**

We take the number of employees directly linked/connected to that particular asset for later calculation of economical range of that asset.

**STEP-4) Risk Calculation**

We then finally calculate the risk based on the previous steps, using the below formula.

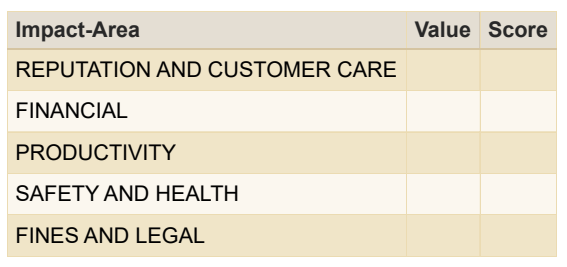
**Risk of that particular impact area = (PRIORITY of that impact area) \* (Average of questions for that impact area).**

**Total Risk = Sum of risks of all impact areas.**

**LOW = 1**

**MEDIUM = 2**

**HIGH = 3**



**STEP-5) Risk Mitigation: - (Add-On)**

We also provide the risk mitigation approach to the user. (Under Research).

Based on the above input we define the coefficient by which we can define the α hence defining the economic range of the asset.

