RISK ASSESSMENT

PROCEDURE POLICY

Table of Contents

1. Objective 4

2. Scope...4

3. Performance Criteria...4

4. Procedure...4

1. Objective

1.1 To identify threats those pose a risk to the information assets at Viraj Profiles Private Limited's

(here after will refer as Viraj Profiles)To determine the probability that noncompliance could occur and not be prevented or detected in a timely manner by the internal controls in place; assess the internal control structure in accordance with ISO 27001.

2. Scope

2.1 To cover all the information assets, activities and services of Viraj Profiles.

3. Performance Criteria

3.1 Finalization of management program and implementation of ISMS.

4. Procedure

4.1 Risk Assessment Plan: Risk assessment will involve following steps:

4.1.1 Identification of business processes

4.1.2 Identification of assets

4.1.3 Preparation of Risk assessment and treatment register

4.1.4 Asset valuation

4.1.5 Identification of threats and vulnerabilities

4.1.6 Estimation of rate of occurrence

4.1.7 Threat impact valuation

4.1.8 Calculation of risks

4.1.9 Categorization of risks

4.1.1 Identification of business processes

4.1.1.1 This step involves identification of business processes and systems that exist at Viraj Profiles

4.1.2 Identification of Assets

4.1.2.1 This step involves the creation of an asset list, per department or project containing the categories as listed below

Types of Assets	Examples
Electronic Assets	Databases, data files, system documentation, user manuals, training material, operational documents, procedure documents, intellectual property, email, reports etc
Paper Assets	Contracts, guidelines, company documentation, business results, purchase documents, invoices, licenses, SLAs, NDAs etc
People Asset	Employees(VP, AVP, Manager, Team Member etc), Contractors, Third Party Vendors
Physical Asset	Computers, Switches, Routers, Hubs, Firewalls, Communication Equipment, Magnetic Media, Back up Tapes, Printers, Telephone Instruments etc
Service Assets	Fire Extinguishers, storage sheds, storage yards, furniture, AC Plant, Telecommunication, ISP, Facilities etc
Software Asset	MS Office, Application, development tools, utilities etc

4.1.3 Asset Valuation

4.1.3.1 Business / financial impact that could occur due to leakage of information asset. (Confidentiality)

4.1.3.2 Business/financial impact if the information asset is corrupted/ altered. (Integrity)

4.1.3.3 Business/financial impact, which could happen due to loss of asset (Availability)

4.1.4 Asset valuation involves determining asset values for all the assets that are identified. These values are measured from the highest parameter of Confidentiality, Integrity and Availability i.e. CIA; on basis of scale VH, H, M or L

4.1.5 Values for Confidentiality, Integrity and Availability

4.1.5.1 The value for CIA can be identified from the scale VH, H, M or L based on the prediction of impact on

4.1.6 Explanation for Confidentiality:

4.1.6.1 For instance, consider a document, which is very confidential for Viraj Profiles (e.g. MSA, SOW) the Confidentiality would be ‘High’ (H) or ‘Very High’ (VH).

4.1.7 Explanation for Integrity:

4.1.7.1 Take an example of an electronic file (e.g. Client SLA, Code) that will have an Impact if its integrity is lost, i.e. if it gets corrupted or altered. Then consider its value to be either ‘High’ (H) / ‘Very High’ (VH).

4.1.8 Explanation for Availability:

4.1.8.1 For example; if you have stored critical data on your local hard-disk which does not get backed up. In case of a disk failure, recovery possibility of your data is low. In that case the value would be a ‘Very High’ (VH).

4.1.8.2 Since Confidentiality, Integrity and Availability for each asset have an equal impact on security; the highest value of the CIA is selected to identify the asset value.

4.1.8.3 Asset:

Asset Scale	Asset Value
VH	4
H	3
M	2
L	1

4.1.9 Identification of Threats and Vulnerabilities

4.1.9.1 This step involves identifying all the possible threats, which can cause the loss of an asset. These threats and vulnerabilities have been identified and an updated list is maintained in ‘Threat Vulnerability and Mitigation matrix’. The threats have to be identified for each asset and listed in the Risk assessment and treatment register.

4.1.9.2 The different types of the threats are:

Types of Threats	Examples
Natural	Earthquakes, Cyclonic storms, etc.
Manmade	Civil Strife/War, Intrusions/Hacking, Virus Attack, Theft, Operator error, deliberate destruction/Sabotage, etc
Technical Failure	Power glitches, Communication link failure, Network component failure, etc.

4.1.10 Estimation of Rate of Occurrence

4.1.10.1 Rate of occurrence (ROO) of the identified threats is estimated on the basis of the past experience. ROO value can be identified from scale ‘VH’, ‘H’, ‘M’ or ‘L’

Rate of Occurrence	Scale	Value
Such an event can occur once in 6 months	VH	4
Such an event can occur once in 1 year	H	3
Such an event can occur once in 1.5 years	M	2
Such an event can occur once in 2 years	L	1

4.1.10.2 For example, in this scale, it is assumed that any threat, which has not occurred form the long time, has a very remote chance of happening, and thus it will be given a value of Low (L) The value shall be entered in the Risk assessment and treatment register

4.1.11 Threat Impact Valuation

4.1.11.1 The goal of this process is to ascertain the impact of threat on the assets identified. The estimation of the level of impact for every threat is made on the basis of past experience using the scale given below:

Level of Impact	Scale	Value
Level of Impact >=80%	VH	4
80%>Level of Impact >=60%	H	3
60%>Level of Impact >=40%	M	2
40%>Level of Impact >=20%	L	1

4.1.11.2 For example, if only half the asset gets damaged because of a threat i.e. the level of impact is 50% and then going by the above table, the value of impact will be taken as ‘M’. The value shall be entered in the Risk assessment and treatment register.

4.1.12 Calculation of Risk

4.1.12.1 Risk is calculated based on:

4.1.12.1.1 Asset value

4.1.12.1.2 Level of impact

4.1.12.1.3 Rate of occurrence

4.1.12.2 Formula used is as below:

4.1.12.2.1 ***Risk faced by the asset = (Asset Value* Level of impact* Rate of occurrence)***

4.1.12.3 Categorization of Risk

4.1.12.3.1 Based on the value of risk calculated, the risk is categorized as Low, Medium, High and Very High as described in table below.

Risk Category	Value of Risk	Action Required
Low	**1< RISK =< 16**	May need some action in long run
Medium	**17=< RISK =< 32**	Need to consider some actions in short term
High	**33=< RISK =< 48**	Some immediate action required including transfer of risk either through outsourcing or insurance
Very high	**69 =< RISK =<64**	Besides Immediate action needs to consider redundancy

4.1.12.3.2 The value shall be entered in the Risk assessment and treatment register

4.1.12.3.3 Once the risk is evaluated, the assets coming in the category of Medium, High or Very High have to be treated in order to reduce or eliminate the risk.

4.1.12.3.4 Assets with a "Risk Value" of 17 (after implementation of existing controls) or more shall be subjected to a risk treatment plan (RTP).

4.2 Risk Treatment Plan

4.2.1 All assets, the corresponding risks and the risk levels, along with the treatment/mitigation plan for each identified asset, will be listed down in the *Risk assessment and treatment register.* Depending on the risk levels, the management shall decide whether the risk to an asset is acceptable or requires treatment (as per policy). One of the following actions is to be taken for treatment of risks:

4.2.2 <u>Reducing the risk</u>

4.2.2.1 Identify appropriate controls for risk levels of Medium, High or Very High to reduce the risk level to Low

4.2.3 <u>Accepting the risk</u>

4.2.3.1 For the risks (except the Low), which cannot be reduced, transferred or avoided due to cost or other constraints, chooses to accept the risk. In such cases where Viraj Profiles has decided to accept the risks that are higher than the acceptance level, (i.e. Medium, High or Very High), an acceptance from the management shall be obtained. The risk valuation greater then 16 (Medium and above) on particular asset needs to be mitigate. However, for all the risks having risk level as Low, it need not explicitly be mentioned, as it is implied that Viraj Profiles will accept those risks and will not mitigate or take any actions against them.

4.2.4 <u>Avoiding the risk</u>

4.2.4.1 Viraj Profiles shall note/identify the risks that can be avoided by adopting preventive methods.

4.2.5 <u>Transferring the risk</u>

4.2.5.1 If it is possible, Viraj Profiles shall identify the risks which can be transferred to other parties such as insurers, suppliers etc.

4.2.5.2 Once the mitigation plans have been mapped against the risks, the Risk assessment and treatment register shall be sent to the Chief Information Security Officer (CISO). The CISO will then prioritize the actions depending on the level of the risk and will identify the high-risk areas as a management program for treating the risks. Viraj Profiles has agreed upon the following timeframes for treating the risks:

4.2.5.3 Very High risks will be addressed within 1 month.

4.2.5.4 High risks will be addressed within 2 months.

4.2.5.5 Medium risks will be addressed within 3 months.

4.2.5.6 After implementation of mitigation/action plan, the rate of occurrence of threat or level of impact on an asset may reduce or may lower down. Hence this is evaluated and a risk value with its risk category is established as per above methods.

4.2.6 **Residual risk**

4.2.6.1 After unacceptable risks have been reduced or transferred, there may be residual risks that are retained. The residual risk statement needs to be approved by management. These residual risks are summarized and reviewed / re-assessed periodically.

4.2.6.2 Risk assessment and mitigation along with threat and vulnerability identifications is reviewed / re-assessed once every six months or as required, to take into account change, such as changes to the organization (e.g. setting up of a new site), technology (e.g. changing the mail server), business objectives and processes, identified threats and in external events (e.g. changes to the legal or regulatory environment and changes in social climate).The residual risk being less than 17 is accepted by the management.