Information Security Risk Management

Confidentiality Statement

The policies, procedures and standard practices described in this manual are for the said process only at SG Analytics **(from here on termed as 'SGA')** and do not extend or imply to any other SGA entity. Information in this document represents guidelines only. SGA reserves the right to modify this document, amend or terminate any policies, procedures, or employee benefit programmes whether or not described in this document at any time, or to require and/or increase contributions toward these programs.

All policies contained herein have been adopted by SGA and supersede previous policies. We periodically review policies, in part or as a whole, to ensure that they continue to reflect current thinking of the organisation and are consistent with trends and legal requirements.

Document Summary

Document Reference #	SGA_PO_Information Security Risk Management_v2.0
Author	Smitha Saju
Reviewed By	Rohit Kalghatgi
Approved By	Susshruth Apshankar
Owner	Rohit Kalghatgi
Document Type	Policy
Document Status	Approved
Document Circulation	Confidential Internal
Document View Level	Internal
Release Date (dd-mm-yyyy)	02-12-2016

Revision History

Version	Date (DD-MM-YYYY)	Author (Designation: Name)	Changes (Short Description)	Remarks
v1.0	09-06-2016	Dy. MR Smitha Saju	-	Initial document
v2.0	02-12-2016	Dy. MR Smitha Saju	-	Reviewed Document

Content

1. Introduction

1.1 Objective

The objective of this document is to describe overall process of Risk Assessment which includes risk assessment, risk assessment report, risk treatment plan and control measurement dashboard.

1.2 Scope

It includes the process for risk management for Information security within SGA.

1.3 Terms and Definitions

Risk: Effect of uncertainty on objectives.
NOTE 1 - Effect is a deviation from the expected.
NOTE 2 - Uncertainty is a state of deficiency of information or understanding.
NOTE 3 - Risk is often characterized by reference to potential events and consequences.

MR: Management Representative

Dy. MR: Deputy Management Representative

ISMS: Information Security Management System

2. Responsibility

Dy. MR is responsible for facilitating risk management.

ISMS Coordinators for departments are responsible for working with risk assessors (Dy. MR) for risk assessment of respective departments.

3. Prerequisite

The guidelines for using the template for Risk Assessment shall be updated within 15 days of each amendment to the template for Risk Assessment.

4. Policy

1. Risk Assessment for ISMS shall be conducted at least once in one year
2. There must be at least one risk assessment later than 6 months and before termination of 12 months from the previous risk assessment
3. All significant risks must be treated within 6 months of risk assessment
4. Risk Owner is the ISMS Coordinator for the respective department
5. Risk Assessment Results must be approved by ISMS Coordinators
6. Risk Assessment Report must be prepared by Dy. MR
7. Risk treatment plan must gather inputs from risk assessment
8. Risk Treatment Plan must be approved by COO prior to its implementation

5. Procedure

1. Dy. MR facilitates risk assessment
2. MR may use competent external organization to perform risk assessment
3. ISMS Coordinators of departments work with risk assessor

4. Following input is taken into consideration during risk assessment:
    a. Needs and expectations
    b. Internal and external context of the organization
    c. Statutory and regulatory requirements
    d. Contractual requirements
5. The response to risks identified are classified or treated in the following ways:
    a. Tolerate: Accept the risk
    b. Treat: Take cost effective actions to reduce the risk
    c. Transfer: By transferring the risk to third party (e.g., by insurance or passing responsibility for the risk to a contractor)
    d. Terminate: Agree that the risk is too high and do not proceed with the project or activity
6. Risk Assessment Results are documented and Risk Assessment Report is prepared
7. Risk Assessment Report is input for Risk Treatment Plan (RTP). RTP describes the tasks, responsibility and target dates for implementation of controls
8. Control Measurement Dashboard is created to measure the ongoing implementation progress of sample of established controls

6. Methodology

1. Before a Risk Assessment is conducted, the following requisites should be checked and ensured:
    a. This guideline is updated to reflect the most recent version of the Template for Risk Assessment
    b. All the participants involved in the Risk Assessment are supplied with a copy of this guideline document
2. Start with the **Context** in which risk is relevant. This will allow the incidents to be categorized as per the nature of impact
3. An aspect taken up for Risk Assessment should be listed in **Activity/Situation**. The aspect could be –
    a. A process / activity within SG Analytics Pvt. Ltd.
    b. A location within the control of SG Analytics operations
    c. Infrastructure, equipment or materials
    d. Changes / proposed changes within the organization

    (This list is indicative. A user of the worksheet may consider any other type of aspect where risks prevail)
4. Identify the **Vulnerability**. Vulnerability is indicative of uncertainty, i.e., a state of deficiency of information or understanding
5. Identify representative **Threat** that may exploit the vulnerability for risk to manifest, i.e., for effect of uncertainty to be visible

6. Indicate what dimension(s) of the **CIA (Confidentiality, Integrity & Availability) triad** the risk would have prominent impact on
7. Determine **Consequence** as follows. Determine the severity of impact the risk may have in the following domains of business:
    a. **Customer Impact**: Does the risk hamper network operation of customer; hamper provision of technical support to customers, or compromise customer's confidential information?
    b. **Product Impact**: Does the risk induce significant development delay or jeopardize integrity of product code?
    c. **Financial Impact**: Does the risk cause significant financial loss to company?
    d. **General Security Impact**: Does the risk cause general loss, compromise or misuse of information not explicitly addressed in above factors?

For each domain, the severity is measured on the scale of 1 to 5, 5 being the highest.

Rating	Description	Customer Impact	Product Impact	Finance Impact	General Security
1	Insignificant	Nil – Negligible	Nil – Negligible	Nil – Negligible	Nil – Negligible
2	Minor	Escalation to analyst	Delay in service delivery by 1 working day	Under $500K	Impact on 1 computer
3	Moderate	Escalation to Manager	Delay in service delivery by 3 working days	Between $500k - $5m	Impact on group of 5 or more
4	Major	Escalation to AVP	Delay in service delivery by 5 working days	Between $5m - $20m	Impact on whole domain/team/department
5	Catastrophic	Escalation to Delivery head/COO/ CEO	Delay in service delivery by more than 5 working days	Above $20m	Impact on whole organisation

The overall consequence is calculated by adding up the severities of impacts on all of the above 4 dimensions and then using the following scale:

Total Impact	Consequence
1-4	1
5-8	2
9-12	3
13-16	4
17-20	5

8. Determine **Likelihood** as follows

Past Occurrence	Likelihood
No incident in past 5 years	1
Up to two incidents in past 5 years	2
More than two incidents in past 5 years	3
Up to two incidents in past 1 year	4
More than two incidents in past 1 year	5

9. Discuss and determine the already **existing controls** that can detect, correct or prevent the incident. List all existing controls that currently address this risk. If no controls exist, then put a dash (-) within the cell

10. Calculate **Individual Control Rating** based on its effectiveness

Effectiveness	Individual Control Rating
Control not exists, not documented, not practices	5
Control not documented, but it's been practice	4
Control is documented and partially implemented	3
Control is documented and fully implemented	2
Control is documented, fully implemented and effectiveness is ensured	1

11. Calculate **Overall Control Rating** as follows:
    a. In case at least one control exists, the control rating will be average of individual control ratings, rounded to nearest integer
    b. If there isn't any existing control, the Overall Control Rating is taken as 5
12. Identify the applicable legal, regulatory or management requirements associated with the risk. If the requirements exist, then select 'Yes' from the dropdown list and also specify the details of the requirement in the next column. If there are no such requirements, then select 'Not Applicable' from the dropdown
13. Risk rating will be automatically calculated in the worksheet. It is a calculated as Consequence x Likelihood x Overall Control Rating
14. SGA has accepted **27 as the risk acceptance criteria**

15. The worksheet will automatically determine the **Significance** based on the following criteria
    a. Rating higher than 27, or
    b. Has at least one regulatory or management requirement associated with it
16. If none of the two criteria listed above are true, then the risk is rated as 'Not Significant'
17. Select any one of the options from the dropdown for **Options for treatment**
18. **Planned Controls** are controls identified to treat Significant Risks
19. Check if the planned controls meet regulatory requirements
20. **Revised Control Rating** is performed as follows:
    a. The rating of planned control will be taken as 1, as it is anticipatory until completely implemented and measured
    b. In case significant risk is not treated by accountable authority due to some reason and top management accepted risk in MRM then revised control rating will follow table given in point number 10 in this document
    c. At the time of next review of risk assessment, revised control rating will be depend on implementation & effectiveness status of related control
21. **Residual Risk Rating** is calculated as follows:
    a. If the Treatment arose out of Risk Rating being higher than 27, then Residual Risk Rating = Consequence x Likelihood x Revised Control Rating, and
    b. If the Treatment arose out of regulatory or management requirement, the control must have met the stated requirement and then Residual Risk Rating = Risk Rating
22. **Acceptable** will be automatically calculated as mentioned below:
    a. marked as Yes , if the planned control meets the legal/ business requirement or the planned control is not applicable or the residual risk rating is less than 27
    b. marked as No, if the planned control does not meet the legal requirement or the residual risk rating is more than 27
23. If the residual risk is not acceptable then further action needs to be discussed and mentioned in **action details**
24. Further action can be taken by following options
    a. Add more controls
    b. Transfer risk
    c. Terminate risk
    d. Tolerate/Accept risk
25. If '**Add more controls'** is selected then it is essential to select controls from Annex A or control defined by the organisation. Further '**Action details**' related to selected additional control need to be updated
26. If '**Transfer Risk**' or '**Terminate Risk**' or '**Tolerate/Accept Risk**' option is selected then update 'Action details'

27. Mention the **responsibility for implementation** ie. task owner and also the **status of the implementation**