Document Title /Name	**Information Security Risk Management Methodology**
Document /Policy Number	ISMS/Pro/006
Current Version	2.0
Document/Policy Owner	Chief Technology Officer, Securitysense
Document Author	Firoz Haider Khan,
Approver	Chief Executive officer /Chief Technology Officer
Effective From	15th March 2012
Next Revision Date	As required
Document Type/Classification	Internal
Document Font	Axiata Book
File Name	Information Security Risk Management Methodology Ver2.0.docx, MS word 2010
Document /File Location	

Document Amendement Records

A =Added, M = Modified, D = Deleted

Version No.	Date	Section No.	A/M/D	Description	Author
Version 1.0	1st October 2010	-	-	1st version.	Firoz Haider Khan
Version 2.0	15th March 2012	-	-	2nd version.	Firoz Haider Khan

Table of Contents

1. INTRODUCTION

1.1 Purpose of Risk Assessment

The purpose of the risk assessment is to identify all susceptibilities to the identified threats, and the nature of the harm that could arise from them.

It is common for vulnerabilities to be countered by safeguards. If an organization can identify the threat and associated vulnerabilities related to any assets then it's easier for the organization to take necessary measures selecting appropriate controls and safeguards.

1.2 Choice of Method and Work Form

1.2.1 Choice of Method

Out of available two risk assessment methodologies, qualitative and quantitative in Information Security field, risk assessment methodology has been chosen for Securitysense Information Security Risk assessment. The reason behind was to point a measurable figures which will help us to know where we are heading and how we are improving.

1.2.2 Work Form

We tried to meet with all related business unit in the Technology Division in the form of face to face interview, meeting, email communication for clarification & review and brainstorming session in the workshop. Head of information security/Network Security and Audit performed necessary inspection to follow-up the process.

1.3 OTHER INFORMATION

1.3.1 Working Party

Name	Unit	Role in the analysis
Firoz Haider Khan	Network Security & Audit	Team Leader
Md. Motashim Billah	Network Security & Audit	Participant of core team
Asif Ahmed	Network Security & Audit	Participant of core team

Table 1: Participants in the working party

2. DESCRIPTION OF SECURITYSENSESECURITYSENSE

Ref: www.robi.com.bd

3. Asset IN SECURITYSENSESECURITYSENSE

3.1 Asset Identification Method

Assets of Securitysense are distributed throughout the country. They are composed of Servers, Storage, Backup media, Network active/passive devices, data center facilities, relevant people and ISMS Documents. Securitysense relates these Assets grouping them into related Services.

Owner of the Assets are identified by the owners of the Service. In general all Technology Services are owned by CTO. Securitysense provided prescribed template is filled by Asset owners to mathematically define the Classification of the Asset.

Finally Asset lists and Classification are approved by Management.

3.2 Asset Classification

In Securitysense Assets are classified in 3 types.

- **Class A**

Mission Critical revenue related applications/servers (Billing, Rating, Mediation, CPS etc.)

- **Class B**

Business Critical but not revenue related applications/servers (Email, SAP, DWH, FMS etc.)

- **Class C**

All Test and Development platform used in Class A and B

3.3 Asset Valuation Method

Considering the business impact and criticality each and every asset will have a numeric value of Confidentiality (C), Integrity (I) and Availability (A). Each of C, I and A value might be varied as per below Table (1) in 4.1. The Asset Value will be derived from the CIA value using below formula: AV = Max (C, I, A)

3.4 CIA Value

5	Very Critical
4	Critical
3	Medium Critical
2	Low Critical
1	Very low Critical

Table 2: Chosen CIA values

4. DELIMITATION OF THE RISK ASSESSMENT

4.1 The Risk Assessment Comprises

The scope of the risk assessment in this document is the assets of type Class A, B and C in Technology Division of Securitysense. This document also covers associated people, facilities, data centers, organization and software.

4.2 The Risk Assessment Does Not Comprise

Any system or process outside of the Technology division, how much critical it might be, is considered out of the scope of this risk assessment.

5. Consequence and Frequency Scales

5.1 Impact Scale

5	Significant and Unrecoverable Revenue Loss, Company image or brand loss.
4	Significant and Recoverable Revenue Loss
3	Significant unavailability but No Revenue Loss
2	Operational and Efficiency Loss.
1	Very low impact.

Table 3: Chosen Impact scale

5.2 Probability Scale

5	Very High, easily predictable
4	Highly probably, foreseen.
3	Medium
2	Low
1	Very Low, Unexpected

Table 4: Chosen Probability scale

5.3 Vulnerability Scale

5	Very High, easily predictable
4	Highly probably, foreseen.
3	Medium
2	Low
1	Very Low, Unexpected

Table 5: Chosen Vulnerability scale

6. RISK REGISTER

6.1 Risk Assessment Template

Risks and threats will be kept in online location using below templates.

Asset Name: <Asset Name>	**Asset Category:** <Software/Hardware /People/Document etc.>	**Asset Owner:** Head of Central Operation
Asset Value, AV: <Asset Value>		
Asset Location:	**Asset Risk Value:** <Asset Risk Value>	**Assessment Date:** 1st October 2008

Threat	**Threat Category**	**Risk Assessment**					**Overall Risk Value for threat**
		Vulnerability	**Vulnerability Value (V_v)**	**Probability (P_v)**	**Impact (I_v)**	**Risk Value (R_v)**	**(R_t)**
Threat-1	A	Vulnerability-1	2	1	4	8	12
		Vulnerability-2	3	1	4	12	
		Vulnerability-3	3	1	4	12	
		Vulnerability-4	2	2	3	12	
Threat-2	C	Vulnerability-5	4	2	4	32	32
		Vulnerability-6	3	1	4	12	
		Vulnerability-7	2	2	2	8	
Threat-3	A	Vulnerability-8	2	2	3	12	12
		Vulnerability-9	2	2	3	12	

Table 6: Risk Assessment Template

Risk Value will be calculated using below formula:

$R_V = V_v x P_v x I_v$

Where

R_v = Risk for any particular Threat due to any particular Vulnerability

V_v = Numeric Value of any Vulnerability

P_v = Probability of particular Vulnerability to occur

I_v = Impact for that Vulnerability

Overall Risk for any Threat is

R_t = Max (R_{v1},R_{v2},R_{v3}....)

R_t = Threat Risk

R_{vn}= Risk for nth Vulnerability

Overall Asset Risk = AV x R_t

6.2 Risk Treatment Template

Risk Treatment Plan will be kept online as per below templates.

Asset Name: <Asset Name>	**/**	**Asset Owner: Head of IT**
Asser Value: <Asset Value>	**Threat Category: C,I,A**	
Asset Location:	**Asset Risk Value: <Asset Risk Value>**	**Assessment Date: <Date>**

ISO 27001 Ref	Threat Category	Control Description
A.x.y.1	A	Description of A.x.y.1 Clause
A.x.y.2	C	Description of A.x.y.2 Clause
...	I	.....

Table 7: Risk Assessment Template

6.3 Risk Mitigation Templates

Plan will be kept online as per below templates.

Asset Name: <AssetName>	**Asset Category: <Software/Hardware/People/Document/Etc>**	**Asset Owner: Head of Development**
Asser Value: <Asset Value>		
Asset Location:	**Asset Risk Value: <Asset Risk Value>**	**Assessment Date: 1st October 2008**

Threat	Threat Category	Risk Mitigation Plan						
		Apply Controls	Cost of Control	Duration	Responsibility	Residual Risk Value	Management Call	Comments
Threat-1	A	A10.1.1, A12.1.1	$120K	6 Month	Head of Central operatio		Accept	

		, A13.2.4			n			
Threat-1	C	A10.1.1 , A12.1.1 , A13.2.4	$130K	1 Year	Head of Central operatio n		Accept	
Threat-1	I	A10.1.1 , A12.1.1 , A13.2.4	No	6 Month	Head of HR		Transfer	

Table 8: Risk Mitigation Template

7. RISK MAP AND RECOMMENDED TREATMENTS

7.1 Risk Map

Risks will be mapped in the above Risk Assessment Templates (Table 6).

7.2 Assessment of Unacceptable Threats

Any risk value greater than 60 will be considered as unacceptable. Concerned Securitysense management still possesses the authority to carry forward or cancel risk treatment or mitigation plat of any asset with any risk value.

7.3 Recommended Risk Treatments

Risk Treatment plan (Table 7) will be approved by the Management and necessary mitigation plan will be carried as per management guideline which will be filled in the templates (Table 8).

8. ENFORCEMENT

This has been made for protection of company assets and employees. Employees have gone through, understood and acknowledged the procedure. All heads of departments will be responsible to enforce this procedure at their level.

9. DISCIPLINARY PROCESS

Any employee or personal found to have violated this procedure may be subject to disciplinary action that will be handled via existing organization governing rules regulation and procedures.

10. REVIEW

Network Security and Audit Team will review this procedure as per need basis in conjunction with major changes to the infrastructure, as part of Securitysense's participation in system security audits, after each breach in system security, or any time if business need.