Procedure for Risk Management Methodology

Athena Global Technologies Ltd.

Document Management Information

Item	Description			
Document Title:	Procedure for Risk Management Methodology			
Document ID:	AGTL-ISMS-SOP-RMM		Version:	1.5
Classification	○Public		▪ Internal	○ Confidential
Status:	Released	Type:	DOC	
Publish Date:	28.08.2024			

Version Number	Date	Author(s)	Remark
1.0	26.08.2019	CISO	Initial baseline
1.1	13.04.2020	CISO	Periodical review
1.2	18.12.2020	CISO	Periodic Review of Information Security related Policies and Procedures
1.3	22.11.2021	CISO	Periodic Review of Information Security related Policies and Procedures
1.4	01.02.2023	CISO	Periodic Review with No Changes
1.5	22.08.2024	CISO	Periodic Review of Information Security related Policies and Procedures with company logo update
Version Number	Date	Reviewer(s)	Remark
1.0	02.09.2019	COO	Reviewed
1.1	20.04.2020	COO	Reviewed
1.2	21.12.2020	COO	Reviewed
1.3	26.11.2021	COO	Reviewed
1.4	06.02.2023	COO	Reviewed

1.5	23.08.2024	COO	Reviewed
Version Number	**Date**	**Approver(s)**	**Remark**
1.0	02.09.2019	CEO	Approved
1.1	20.04.2020	CEO	Approved
1.2	21.12.2020	CEO	Approved
1.3	26.11.2021	CEO	Approved
1.4	06.02.2023	CEO	Approved
1.5	28.08.2024	CEO	Approved

TABLE OF CONTENTS

1.0 PURPOSE

- To maintain uninterrupted services towards Athena clientele
- To ensure the risks are kept under control to accepted and minimal levels as identified by Athena and by doing so ensure optimum efficiency levels of business operations at Athena
- To ensure the controls are put in place to mitigate the unacceptable risks as per Athena standards and hence ensuring the preparedness to tackle the impacts from the risks

2.0 SCOPE

The scope of risk assessment is defined in the ISMS scope document of Athena (Please refer ISMS manual Section-1 for scope)

3.0 POLICY

The senior management of Athena is committed to ensuring that the procedures are in place for monitoring Risk Management. This is ensured through training across the organization and monitoring the implementation from time to time

4.0 PROCEDURE

4.1 Risk Assessment Approach

- Athena's approach to risk assessment is to ensure that all assets, to include, information, paper, software, hardware, people and services are identified, evaluated, threats and vulnerabilities identified, risk measured and controlled in a graded manner, so as to improve the overall quality of services to the client thus resulting in better performance
- The Risk should be measured on a single scale, such that risks to different assets can be measured on the same scale and decisions taken in the light of the impact on business. The Risk Analysis should enable the management to take informed business decisions for treatment, transfer, termination and avoidance of the specific risk
- Risk Criteria: The acceptance of risk will be based on the following factors
- During the initial Phase, i.e. first two years, the Risk Criteria will be based on the existing organisational requirements and structure. Risk will be managed by implementing suitable policies and procedures within the existing system, to ensure operational efficiency. Risk Assessment will be carried out by using a Qualitative Process
- Thereafter once decided by the ISMS Committee, that the ISMS is stabilised, the Risk Criteria will be based on the effect of the risk and will be more proactive in nature. The Qualitative Process shall include Quantitative aspects of Risk also
- The Risk Criteria will take into account legal, regulatory and contractual requirements. The same shall be coordinated by the ISM through the Athena's ISSC committee that handles ISMS implementation
- The Risk Assessment is defined as the overall process of risk analysis and risk evaluation
- Risk analysis is defined as the systematic approach to identify an organization's exposure to uncertainty and to estimate the risk
- Risk evaluation is defined as the process of comparing the estimated risk against given risk criteria to determine the significance of the risk
- This document provides details about the risk assessment process for Athena

4.2 Risk Assessment Process

The risk assessment in the Athena is carried out as per the following steps:

- Identification of Assets and their owners
- Ascertaining their location (physical and logical location)
- Evaluation of Assets
- Identification of threats and the corresponding vulnerabilities pertaining to the assets identified above
- Evaluation of threats and vulnerabilities identified above
- Evaluate the probability of occurrence of the identified threat
- Calculate the impact of the occurrence of a threat and express it through a Risk Rating
- Identification of risk owners.
- Select controls for treatment of risk.
- Identify and evaluate options for risk treatment.
- Approval from risk owners for selected controls implementation and for residual risk.

The Risk Assessment Process has been represented pictorially below

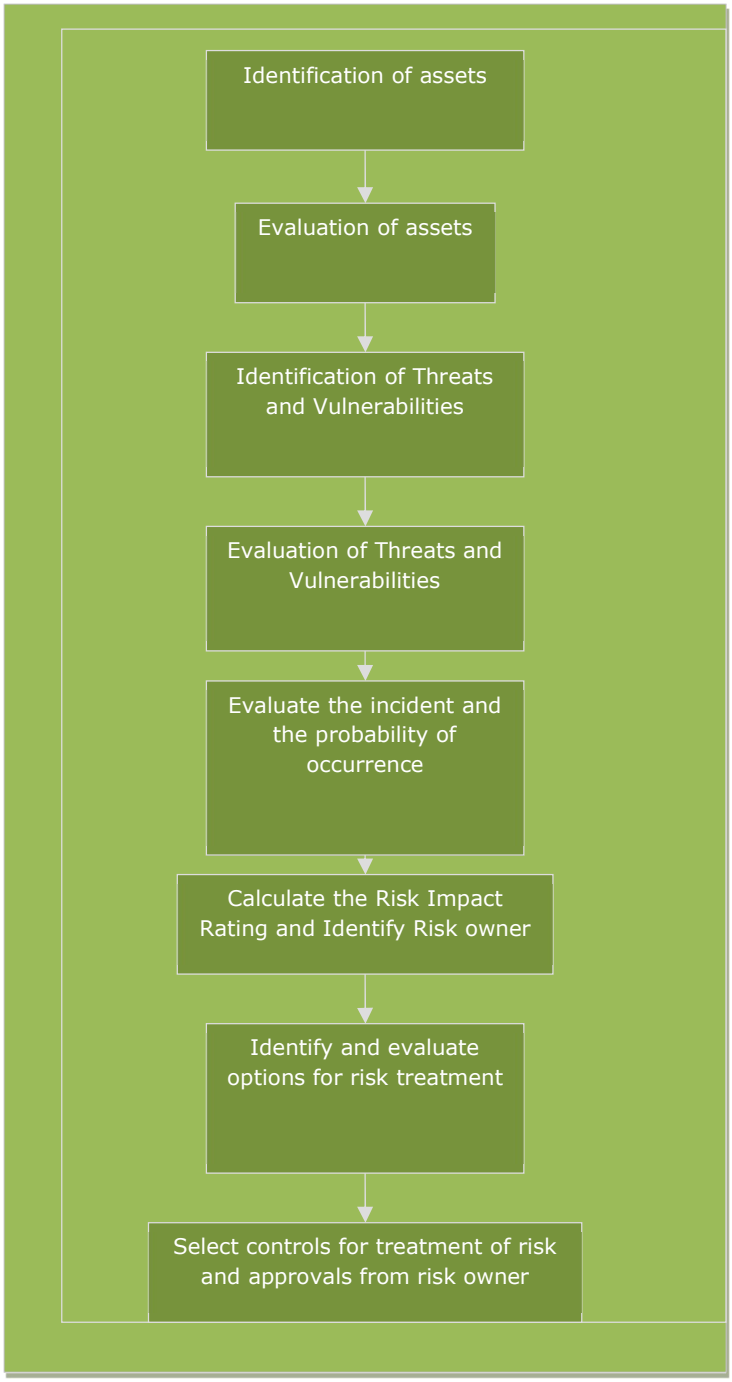

Figure 1: Pictorial Representation of the Risk Assessment

4.3 Identification of Assets

The following guidelines shall be used for identifying assets:

- An asset is something that has value or utility to the organization, its business operations and their continuity. Asset identification and valuation based on the business needs of Athena is a major factor in the risk assessment process. The assets should be identified by individual department members and the list ratified by the head of the section
- As is recommended by the ISO-27001:2013 Standard, Athena uses a Process Based approach for identifying the assets. The same has been depicted pictorially below:

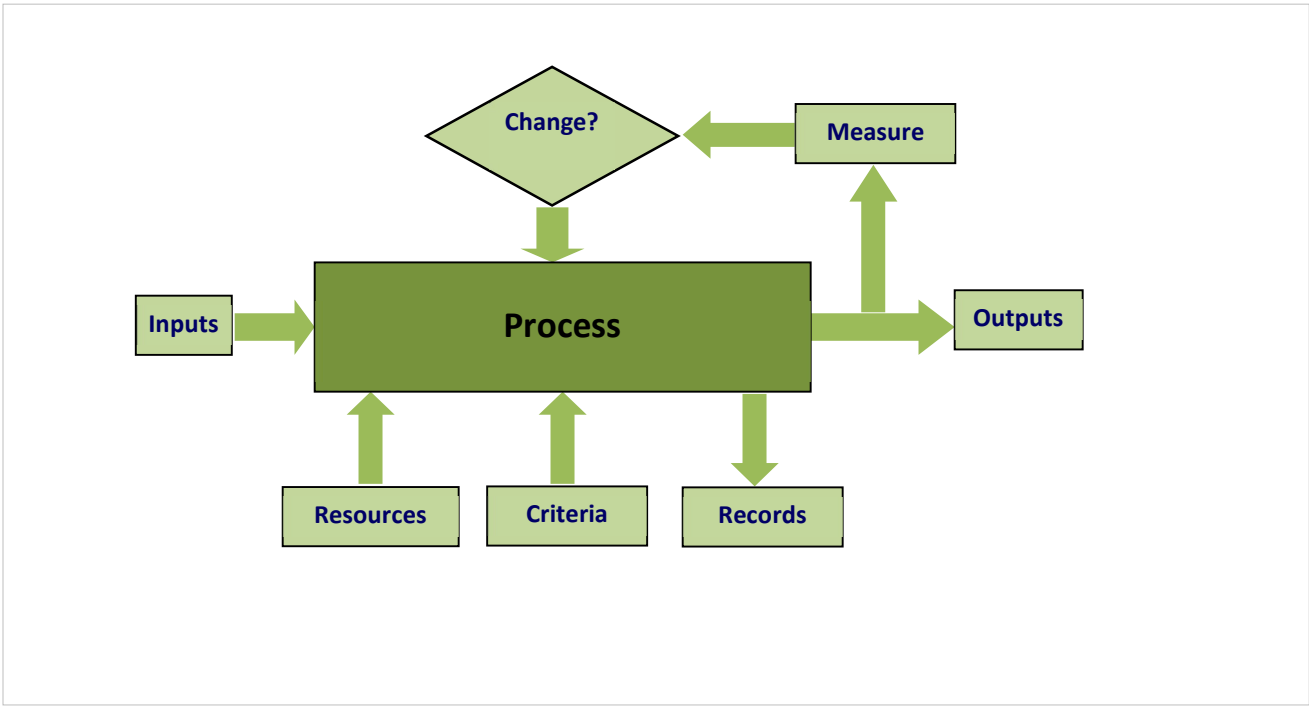

Figure 2: Pictorial Representation of the Process Approach

Note: Resources in Figure 2 may be defined as items required for the completion of the process. These could be in terms of physical assets, time, and money required for completion of the tasks. The physical assets can further be divided into various forms like paper assets, human assets, hardware and software assets, backups, services, and several other such categories. These can be broadly termed as the information assets as they will be either holding information, processing information or would be indirectly protecting the assets holding/processing the information related to the organization

The Process Approach involves the following Activities:
Identify business functions within the Scope of the ISMS. (Refer Figure 2 above)
Analyze individual processes/activities performed by the business function to identify the following parameters of the process:

- Input(s) to the process (e.g. statement of requirements, objective, information inputs, etc.)

- Resources required for executing the process (e.g. manpower, technology, equipment, environment, communications, etc.)
- Criteria defining the boundaries of the process (e.g. legislative requirements, customer specifications, corporate policies and procedures)
- Records generated as part of the process (e.g. receipts, transaction data, complaint forms, authorization forms, etc.)
- Output(s) of the process (deliverables of the process)
- Records of the measured output (e.g. audit reports, internal verification check, quality control, etc.)

List the parameters containing information as information assets and the resources from these parameters as assets to the process
List the owner and custodian of each of the identified assets within the scope of the ISMS
List the quantity of each asset
Create an inventory of assets, listing the owner, custodian, location and the quantity held.
Grouping of Assets:
All similar assets shall be grouped together for the process of the initial risk assessment. For e.g. Notebook PCs having the same asset value shall be grouped together. This analogy shall be extended to all other categories of assets as well
Changes in the Asset Value due to changes in Process Value may require the ungrouping of the Assets in subsequent Assessments

4.4 Evaluation of Assets

The following guidelines shall be used for evaluating the assets:

- In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business or their potential value under different circumstances
- The following seven categories of assets, as listed in the "Asset Register", shall be consider for risk assessment
  - Image and Reputation
  - Digital Information
  - Paper Documents
  - People Assets
  - Physical Assets
  - Service Assets
  - Software Assets

- The input for the valuation of assets, particularly information, should be provided by owners and users of the assets
- The confidentiality, integrity and availability requirements of an asset are to be scored using the following four-point scale:

Level	Score	Explanation
Very High	4	This asset has the highest value in the process. Its loss or destruction could have an immediate and severe impact on the process's viability. It would seriously impact the organization in terms of business activities, financial loss or loss of business
High	3	This is an asset which is extremely valuable to the business process and its loss or destruction could have a severe impact on the process viability and disrupt business activities
Medium	2	This is an asset which can be replaced but the loss or destruction of the information asset would have an immediate impact on business profitability
Low	1	This is an asset which is replaceable. There would only be a low impact on overall business profitability

- Asset Value should be derived by taking the highest of the CIA values (Confidentiality value, Integrity Value and Availability Value as arrived as per above table).

4.5 Identification of Threats and Vulnerabilities

The following guidelines shall be used for identifying the Threats and Vulnerabilities:

- A threat has the potential to cause an unwanted incident which may result in harm to a system, process or organization and its assets. This harm can occur from a direct or indirect attack on the organization's information assets and its resources. Threats can originate from accidental or deliberate sources or events
- Vulnerability may be defined as a weakness associated with an asset, which exposes the asset to different threats. This weakness could be because of an inherent attribute of the asset, the process, the business or the environment. These weaknesses may be exploited by a threat causing unwanted incidents resulting in loss or damage to the assets. It is important to understand that vulnerabilities by themselves do not cause any harm. It is merely a condition, or a set of conditions that may allow a threat to affect an asset
- Asset owners and users should list the different threats and vulnerabilities to the assets
- The vulnerability identification procedure should identify the weaknesses in the physical environment, personnel, management, administration procedures and controls, hardware, software or communications equipment and facilities. This procedure is also applicable to the processes

4.6 Evaluation of Threats and Vulnerabilities

The following criteria are to be applied when evaluating the threats:

Level	Score	Explanation
Very High	4	Incidents at this level can be devastating and need an immediate and appropriate response. Significant potential financial losses, coupled with a public loss of credibility are all symptoms of this type of incident • Could lead to bankruptcy • Could lead to the organization being closed down • Threaten the future of the business • Widespread and serious embarrassment or distress
High	3	Critical incidents are those from which you should be able to recover. With careful management of the incident and the implementation of appropriate safeguards, a 'medium' financial loss and public embarrassment are likely to be experienced • Causes serious disruption/financial loss • Serious breach of legal or regulatory requirements, • Seriously affect relations with the customers or share holders • Serious embarrassment or Distress
Medium	2	The impact of a controllable incident is likely to be short term and is controllable. With the right safeguards and response, the impact could perhaps be reduced to minor embarrassment and minimal cost • Detrimental to Business efficiency or financial health • Technical breach of a Legal or Regulatory business • Adversely affect relations with customer & shareholders • Minor embarrassment or distress to an individual
Low	1	Incidents classified as irritating are likely to be ephemeral and generally will result in little more than a localized irritation. Whilst you safeguard against them, they should be straightforward to avoid and manage • Little or no Disruption or Financial loss • No legal or Regulatory Obligation • Minor & Limited embarrassment within the organization • No distress or Embarrassment within the organization

Example:
A threat like failure of communication lines during business hours will lead to a loss of productivity. Hence, the threat is rated as high or highest, a threat like system (desktop) failure will cause some disruption to business, but the damage would not be large hence the threat is rated as medium or low

The following criteria are to be applied for evaluating vulnerabilities:

Level	Score	Explanation
Very High exposure of asset	4	This vulnerability is an inherent weakness of the asset causing the highest exposure factor for the asset increases the probability of occurrence from Medium to Very High increases the probability of occurrence from High to Very High remains the same when probability of occurrence is Very High
High exposure of asset	3	This vulnerability is a weakness caused due to the procedural, customer or business requirements, causing a high exposure factor for the asset increases the probability of occurrence from Low to (a) High or (b) Very high increases the probability of occurrence from Medium to (a) High, severity is very high
Medium exposure of asset	2	This vulnerability is a weakness causing medium exposure for the asset. This will predominantly include assets that do not have a severe effect on the process increases the probability of occurrence from Very Low to (a) High or (b)Very High increases the probability of occurrence from Low to Medium
Low or minimal exposure of asset	1	No Vulnerability identified OR Identified Vulnerability has no effect on the probability of occurrence.

4.7 Evaluation of Impact

The following process shall be used for evaluating the Incident:

- A vulnerability and threat together result in Impact; this causes a risk factor for an asset and hence the incident shall have a single numeric value as calculated below:
- Impact = Asset Value * Threat Value * Vulnerability Value
- When talking about risk, it is difficult to address a vulnerability or threat in isolation

ImpactValue

Impact severity Matrix (*impact* = *asset value* x *threat value* x *vulnerability value*)

		Threat Value	**Low**				**Medium**				**High**				**Very High**			
		Vulnerability Value	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**	**L**	**M**	**H**	**VH**
	Asset Value	**Low**	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
		Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
		High	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
		Very High	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

4.8 Evaluation of the probability of Occurrence

- The following criteria are to be applied when calculating a rating score for the Probability of Information Security Incidents:

Level	Score	Explanation
Very High	1.0	The incident has a very high probability of occurring unless corrective action is applied A highly event that could be reasonably expected to occur at least every month or more frequently.
High	0.75	The incident has a high probability of occurring unless corrective action is applied. An event that is highly probable, and could be expected to occur several times a year (BUT NOT EVERY MONTH i.e. >1 &<12)
Medium	0.50	This is considered to be a reasonable probability that this incident will occur if corrective action is not applied. An event likely to occur relatively infrequently, perhaps once a year.
Low	0.25	This is considered to be a low probability that this incident will occur. An event that is highly unlikely to occur, if ever or An event that is unlikely to occur, perhaps once every 3 years

4.9 Calculation of Risk Rating

Determine risk of an asset on an entity or organization that affects the way in which business is conducted

	Low	Medium	High	Very High
Asset value (Based on C-I-A)	1	2	3	4
Threat value	1	2	3	4
Vulnerability value	1	2	3	4
Likelihood	0.25	0.5	0.75	1.0
Risk Value	0.25 - 16	16.25 - 32	32.25 - 48	48.25 - 64

For example;

Risk Value is Very High if it comes in between 49- 64

e.g if Asset Value, Vulnerability value and Threat value is 4 , 4 and 4 respectively.

then Impact Value would be 4 * 4 * 4 =64and if Likelihood is 1

then

Risk Value become Likelihood * Impact Value

i.e. 64 *1 = 64, which is considered as very high

Risk Rating

Risk Rating	Risk Value
Very High	48.25- 64
High	32.25 – 48
Medium	16.25 -32
Low	0.25-16

- Risk rating will help in the prioritization of risk treatment. Acceptable risk level is based on the above scale
- The Risk Rating is calculated according to the following formula:

  Risk Rating (RR) = Impact Value * Probability of Occurrence

- To calculate the Risk Rating it is necessary to multiply each of the Risk Rating Components with each other. Higher the resultant score - the higher the Risk Rating. The highest Risk Rating on this basis is therefore 64 {i.e.4*4*4*1}, with the lowest possible Risk Rating being 0.25 {i.e 1*1*1*0.25}
- The Risk impact rating helps us to prioritize the risk into three different levels:
- Very High, where the RR ranges from 48.25 – 64 (i.e 48.25<RR≤64)
- High, where the RR ranges from 32.25 - 48 (i.e.32.25<RR≤48)
- Medium, where the RR ranges 16.25 - 32 (i.e. 16.25<RR≤32)
- Low, where the RR ranges from 0.25- 16 (i.e. 0.25≤RR≤16)

Acceptable Risk Value	Risk value between 0.25 to 16

4.10 Guidelines for Identifying Impact

The ISO 27001: 2013 gives the following definitions:

Confidentiality – Ensuring that information is accessible only to those who are authorised to have access

Integrity – Safeguarding the accuracy and completeness of information and processing methods

Availability –Ensuring that authorised users have access to information and associated assets, when required

An incident would directly impact the Confidentiality, Integrity or availability requirements of a particular asset

It is important to identify which aspect of the CIA (Confidentiality, Integrity and Availability) triad is affected. An incident could result in the loss of Confidentiality, Integrity, Availability or a combination of the three

4.11 Guidelines for Identifying Existing Controls

- The Risk Rating gives an insight into the overall impact due to the occurrence of a particular threat that the asset is exposed to. The next step is to identify the existing security controls which have already been implemented
- These controls help us to identify the current level of risk faced by the organization. The asset owners and users should list the existing controls against each incident that has been identified and list the existing level of risk as low, medium or high. The criteria for identifying whether the existing risk level is low medium or high is as follows:

Low	Asset exposure is minimal after considering existing controls
Medium	Asset exposure is medium even after application of existing controls. The existing controls do not address the incident and asset completely
High	Asset exposure is high even after application of existing controls. The existing controls do not address the incident and asset.
Very High	Asset exposure is very high even after application existing controls. The existing controls do not address incident and asset.

- The identification of existing controls will enable the organization to focus its corrective measures towards those threats which are associated with the highest Risk

4.12 Guidelines for Risk Treatment

All risk items above the acceptable level of risk are chosen for risk treatment. These items can be used to take informed business decisions for treatment, transfer, termination and avoidance of the specific risk

- **Avoided / Terminated** – In this case the vulnerability itself is removed or replaced
- **Treated** – controls are implemented to reduce the level of risk
- **Transferred** – The liability is transferred to an external entity through an agreement. An insurance policy is one such example
- **Tolerated/Accepted** – The management decides that it is ready to accept that risk, because of business limitations. They might address the issue when appropriate resources are available
- The process owners should clearly identify the corrective action to be taken, individual responsible for the activity, assign timelines and request the management for appropriate resources (finance, manpower, and infrastructure)
- Once the corrective activity has been determined and implemented, the new Risk level should be calculated to check whether the applied control has mitigated the risk to a level that the management has agreed to tolerate
- The risk status of the information assets prior to corrective activity is called 'Existing Level of Risk' and the status after corrective activity is called 'Residual Risk'
- For an incident if the RR value is from 0.25 to 16, then no controls are to be selected for the risk mitigation as this is the acceptable level of risk (refer methodology defined above). If the value of RR is 16.25 or above suitable controls for risk mitigation will be selected and implemented
- After carrying out the quantitative analysis of the risk pertaining to the assets, controls are selected for the mitigation of the risk. Once the controls are implemented, risk is calculated qualitatively. If the selected controls have met their desired objectives in treating the risk, the Residual Risk is termed as low; else it would high and would have to be mitigated
- The risk that the organization carries with regard to the threat to its information assets is the result of a combination of factors. Any change to any of these factors will alter the risk profile. This necessitates reviewing and undertaking the complete risk assessment process on a regular basis to ensure that the safeguards employed continue to offer the appropriate level of protection.

4.13 Review of Risk Assessment

- The Risk Assessment will be reviewed at least once every six months. More frequent reviews shall be undertaken in the following circumstances:

- Major changes in Assets or circumstances, e.g. shift of high value assets from one location to another with different physical, administrative or logical parameters
- Changes in layout, design of networks, thus changing the utilisation of the assets
- Changes in Legal, Regulatory and Contractual requirements
- Changes in the organisation structure, thus affecting major changes in policies and procedure