Cogent Private Limited

Monitoring, Measurement, Analysis and Evaluation

Policy and Procedure

Based on ISO/IEC 27001:2013

Version: 3.2

Preface

The Cogent E Services Private Limited (hereafter referred to as "Cogent") Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent ISMS Team welcomes and solicits feedback from users of this document and its reference artifacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis. This document forms part of Cogent's ISMS Policy framework and as such, must be fully complied with. It states the steps Cogent will take to limit the opportunity for information leakage by implementation of best practice, processes and procedures.

Document Revision History

Version	Prepared by		Reviewed by		Approved by		Implementation Date	Summary of Changes
	By	Date	By	Date	By	Date		
0.1	ISM	03rd Dec'14	CISO	05th Dec'14	ISSC	--------	---------	Initial Draft
1	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	First Revision
1.0	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	New Template and updated document
1.1	ISM	13th Nov'15	CISO	13th Nov'15	ISSC	13th Nov'15	2nd Jan'16	
1.2	ISM	15th Oct'16	CISO	15th Oct'16	ISSC	15th Oct'16	31st Dec'16	
2.0	ISM	15th dec'17	CISO	15th dec'17	ISSC	15th dec'17	1st Jan'18	
2.1	ISM	22nd dec'18	CISO	22nd dec'18	ISSC	22nd dec'18	3rd Jan'19	
3.0	ISM	07th Dec'19	CISO	07th Dec'19	ISSC	07th Dec'19	10th Dec'19	
3.1	ISM	07 Jul'21	CISO	07 Jul'21	ISSC	07 Jul'21	11th Jul'21	
3.2	ISM	07 Apr'22	CISO	07 Apr'22	ISSC	07 Apr'22	11th Apr'22	

Copyright

This document contains proprietary information for Cogent. It may not be copied, transferred, shared in any form by any agency or personnel except for authorized internal distribution by Cogent, unless expressly authorized by Cogent Information Security Steering Committee in writing.

Document Distribution

The Cogent Chief Information Security Officer (CISO) shall distribute this document to members of Information Security Steering Committee (hereafter referred to as ISSC) and

Information Security Implementation Committee (hereafter referred to as ISIC).

*The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet server at location http://********

The CISO will ensure that any update to the Cogent ISMS is incorporated on the intranet server and is communicated to all employees of Cogent through an appropriate mode such as e-mail.

Distribution List

Name	Acronym
Information Security Steering Committee	ISSC
Information Security Implementation Committee	ISIC
Chief Information Security Officer	CISO
All employees and relevant external parties.	-

Conventions

The statements containing the words 'shall' and 'required to' in the document are mandatory rules. Failure to observe these rules may be construed as non-compliance to the policy.

The statements containing the words 'should' and 'recommended' imply a desirable requirement. Failure to adhere to these rules may not be a direct non-compliance.

Table of Contents

1. Overview

The ISO/IEC 27001:2013 Standard Clause 9.1 Monitoring, measurement, analysis and evaluation states that "The organization he organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
c) when the monitoring and measuring shall be performed;
d) who shall monitor and measure;
e) when the results from monitoring and measurement shall be analysed and evaluated; and
f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.
NOTE The methods selected should produce comparable and reproducible results to be considered valid.

2. Purpose

This Cogent E Services Private Limited (hereafter referred to as "Cogent") procedure describes the overall requirements for monitoring and measurement as part of Cogent's ISMS requirements to ensure that there is adequate control on ISMS aspects, compliance with legal and other requirements, and to ISMS achieve objectives and targets
The purpose is to establish a consistent process for monitoring and measuring the key characteristics of the organization's activities, products, and services (e.g., processes), that contribute to significant to its Information Security Management System and for ensuring that equipment used to monitor/measure performance related to these processes is properly calibrated.
The intent of such monitoring and measuring is to track ISMS performance, assess implementation and effectiveness of operational controls, and track performance on objectives and targets of the Information Security Management System of Cogent.

3. Scope

All employees, contractors, part-time and temporary workers, service providers, and those employed by others to perform work on Cogent premises, at hosted or outsourced sites supporting the Cogent , or who have been granted access to Cogent information or systems, are covered by this procedure and must comply with associated standards and guidelines.

This procedure includes planning, execution, reporting and follow–up and applies to all departments that form part of the company Quality & Information Security Management System

4. Normative Reference

The following referenced documents are indispensable for the application this policy. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies on ISO/IEC 27001:2013, Information technology – Security techniques – Information management systems – Requirements.

5. Responsibility

1. **Chief Information Security Officer(CISO)**
   a. Organizing Internal Audits, monitoring and measurement activities management review meetings,
   b. Reporting on performance of Information Security Management System
   c. Improve Information Security efficiency and Information Security saving through maintenance and behavior changes by your own employees
   d. Take follow up actions for ensuring continual improvements
2. **The Information Security Manager** performs the risk assessment to identify the type and level of audit logging and monitoring that might be required for each individual information asset.
3. **Owners of individual assets** are responsible for identifying and agreeing with the Information Security Manager the logging and monitoring capabilities of the assets they own and for having them configured to meet the requirements of the risk assessment.
4. **The Quality Manager** is responsible for ensuring that the required monitoring activity takes place using, where necessary, outside contractors to confirm that configuration is in line with requirements of this procedure.
5. **The Head of IT** is responsible for configuring the information systems to meet the requirements of this procedure.

6. Policy Statement

"Cogent will establish an effective Measurement, Analysis and Evaluation Procedure to regularly audit its ISMS and maintain appropriate protection of organizational assets."

7. Procedure

The CISO, in consultation with the ISSC and the executive responsible for relevant projects / functions / departments if necessary, shall establish monitoring criteria in the following areas:

i. The achievement of ISMS objectives and targets and the progress of programmes.
ii. The effectiveness of operational control procedures for controlling the significant ISMS aspects of project activities including the control and monitoring of contractors' ISMS performance.
iii. The conformity of legal requirements and other requirements related to Cogent ISMS .

After an objective and target is developed and approved, Information Security Management Plans (ISMPs) are created to specify the implementation details. These details are further described in the Objectives, Targets, and Management Programs Procedures.

Performance indicators (Pis) are assigned to each associated objective and target and are developed to monitor the key characteristics relative to the objective and target.

As new projects arise or existing activities change, the affected Department will review the projects/activities to determine if new monitoring and measurement requirements are needed and adjust their performance indicators if appropriate.

The CISO compiles PI data and provides periodic updates to senior management at annual review meetings. It will include specific details on:

- What parameter to monitor and measure.
- How such measurement is to occur (including frequency).
- Record keeping.
- Reporting of measurements, including deviations from normal operations.
- Reference to appropriate calibration of equipment, as necessary.

Certain monitoring equipment is used to monitor operations that have an Information Security impact. Calibration of this equipment is managed and maintained by the affected department.

Resources

The CISO shall ensure appropriate resources (financial, human, technological) are available to monitor and measure the selected parameters.

Training

The CISO shall ensure training is provided on monitoring and measurement methods

Collection of Data

The CISO shall ensure that the Monitoring & Measurement data from the identified activities, products, and services is collected. This report could include initial data to establish baseline conditions for future comparison, and would be structured as a minimum to:

- Provide status of Information Security Management Programs designed to fulfill Information Security Objectives & Targets.
- Provide status of performance indicators as related to targeted timeframes,
- Provide compliance status of Information Security operating permits issued by Information Security regulatory agencies.

Performance Tracking

Information Security data collected to reflect Information Security performance is to be maintained in such a manner to allow the evaluation of progress toward realizing Information Security Objectives & Targets.

Regulations, Laws and Other Requirements

Ensure that compliance regulations, laws and other requirements are monitored. This will be accomplished by conducting a Compliance Audit every year

Key IT Systems Parameter/s that are to be measured and recorded are:

a. Audit logging

The servers/systems/devices for which user activity audit logging is configured,and the audit logging software that is deployed together with the schedule/matrix of audit log requirements and reporting regularity are set out in a table in appendix below.

System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured.

The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.

The following data protection or privacy protection restrictions also apply:

(

Commented [h1]: ,(Rajneesh Please Update)

b. Monitoring system use

The servers/systems/devices for which user activity monitoring is configured, together with the schedule/matrix of monitoring requirements and reporting regularity are set out in table in appendix below.
System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured.
The schedule/matrix of monitoring requirements and the monitoring reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.

Monitoring reports are reviewed at define regularity and responsibility. Any evidence of system misuse is reported to the Information Security Manager who investigates further, and the disciplinary process may be invoked.

c. **Protection of log information**

Audit logging is configured as set out above.
Administrators are prohibited from disabling logging activity; disabling audit logs or tampering with audit log information is treated as a serious offence in the disciplinary policy and may result in immediate dismissal.
Describe how system logs and event types are investigated, what tools might be used, etc .
Describe how system logs are securely stored and archived

Commented [h2]: ,(Rajneesh Please Update)

d. **Administrator and operator logs**

The servers/systems/devices for which administrator/operator activities are logged and the logging software that is deployed together with the schedule/matrix of administrator and operator activity log requirements and reporting regularity are set out in a table in appendix below.

Commented [AC3]: If you deploy an IDS or other monitoring tool, you should reference from here its configuration and reporting procedures

System administrators are prohibited from erasing or de-activating logs of their own activities and the technical configuration of this control is ensured .
The schedule/matrix of activity log requirements and the log reports are classified as confidential information and must be handled in line with the requirements of this ISMS for handling confidential information.
The following data protection or privacy protection restrictions also apply
Describe how administrator and operator logs and event types are investigated, what tools might be used, etc .

Commented [AC4]: This clause must reflect any local legal requirements around this sort of data.

Commented [h5]: Rajneesh Please Update)

e. **Fault logging**

The Organization deals with error and fault logging as follows:
Here you should insert details about how you deal with these issues,

Commented [h6]: Rajneesh Please Update)

f. **Clock synchronization**

The clocks of all information systems within Cogent or if necessary specify in a schedule different points of synchronization for geographically dispersed systems are synchronized with specify what and how the synchronization is performed across the network .

Commented [h7]: Rajneesh Please Update)

Throughout its information systems, the date stamp format used by Cogent is: dd/mm/yyyy. The timestamp format used by Cogent is hhmm, applying the 24-hour clock.

Commented [h8]: Rajneesh Please confirm)

Commented [h9]: Rajneesh Please confirm)

The clocks on all servers and all Organizational information processing devices (including laptops, PDAs) are checked on a regularity? Basis how and by whom ? and corrected where necessary.
The record of completed checks and any necessary corrections is forwarded to the Head of IT .

Commented [h10]: Rajneesh Please Update)

Monitoring and measuring allows decision makers to determine whether or not a specific process is operating within specific parameters and, if not, where changes need to be made in the process to achieve the desired level of performance.

In considering what to measure/monitor relative to ISMS performance there are generally three categories of requirements that should be considered:
1) things that are monitored through taking quantitative measurements
2) things that are monitored through a single assessment, and
3) things that are monitored through examining trends (i.e., progress toward achieving objectives and targets).

1.To this end, the Corporate Information Security Officer (CISO), or their designee, will develop and maintain a **Master List of All Monitoring and Measuring Requirements**, particularly the examination of progress toward achieving objectives and targets.

The Master List of Monitoring and Measuring requirements is intended to be a "living document" in that it should be updated whenever new requirements are discerned throughout the ISMS cycle.

2.In developing the list, the Corporate Information Security Officer (CISO) should consider the various objectives, targets, tasks, and requirements specified in the various Management Programmes (MPs), as well as requirements related to the maintenance of operational controls. In addition, the Corporate Information Security Officer (CISO) should consider any underlying activities that "feed into" the processes being monitored/measured to determine if monitoring/ measuring at these subordinate levels will enhance the ability of the organization to make better and more informed decisions regarding its performance.

At a minimum the master list of monitoring and measuring requirements shall include the:

- Measurement criterias from which the monitoring/measuring requirement is derived;
- Parameters and/or processes being monitored/measured;
- Frequency of measuring/monitoring;
- Person responsible; and
- Location of the appropriate record.

3. Periodically, but at least once each ISMS cycle, the Corporate Information Security Officer (CISO)and others, as appropriate, will review the master list of monitoring and measuring requirements to determine if it is sufficient to adequately track the performance of the ISMS and/or to make adequately informed decisions about the organization 's performance.
If it is determined that additional monitoring and/or measurements are needed, the Corporate Information Security Officer (CISO) will work with the appropriate manager responsible for the process to develop the indicator and then add it to the Master List.

4. The Corporate Information Security Officer (CISO), or their designee, shall develop a master list of all equipment that requires calibration and is used to monitor/measure performance within the organization's ISMS (an ISMS document).

This list shall include the name, manufacturer, model number of each piece of equipment; the frequency of calibration; when the last calibration was completed and when the next is due; who is responsible for the calibration; and the location of the calibration record.

The list of equipment requiring calibration should be reviewed and updated whenever the Master List of Monitoring and Measuring Requirements is reviewed to ensure any new equipment is identified and added to the calibration list. In addition, the Corporate Information Security Officer (CISO) should contact the person(s) responsible for ensuring equipment calibrations are completed as needed to update the list with new last and next calibration dates.

6. Monitoring criteria shall include the monitoring / measuring frequency, methods, responsibilities and records or reports that shall be kept. The monitoring criteria shall be documented or integrated into the respective operational control procedures (refer OCP's)

The responsible Project / Function / Departmental Manager shall ensure that the monitoring requirements are carried out and report any ISMS nonconformities to the Corporate Information Security Officer (CISO).

7. The ISSC shall hold regular meetings (approximately every 3 months) and maintain records to:

Commented [h11]: Nitin Please decide frequency

I. discuss and review the achievement of the objectives and targets and the progress of relevant programmes;
II. review the monitoring data (e.g. inspection checklists) to check whether the monitoring and operational control procedures are implemented properly;
III. review information to evaluate whether Cogent activities comply with applicable ISMS legislation and other requirements identified ;
IV. review any ISMS nonconformities, and the corresponding corrective action and preventive action

In case of nonconformities, the relevant Project / Function / Departmental Manager shall investigate the causes of nonconformities and establish appropriate corrective and preventive actions. The corrective and preventive actions shall be verified by the Project / Function / Departmental Manager and endorsed by the CISO).

The monitoring criteria shall be reviewed and revised according to changes in legislative requirements and the practical situations of Cogent 's a result of continual improvement of ISMS performance. Whenever necessary, calibration of measuring equipment shall be defined clearly in terms of calibration methodology, calibration frequency, acceptance criteria and responsible personnel.

Cogent shall record the results (and maintain the records) of the periodic evaluation of compliance and shall be considered at the management review.

Process Inputs:

S. No.	Input	Source	Frequency	Reference
a.	Management Review Records	MR	3 Month	
b.	Maintenance Records	Head Maintenance	Monthly	
c.	Supplier Performance Records	Head Purchase	3 Month	
d.	Product & Process Performance Record	Head Production	3 Month	
e.	Internal Audit Records	MR	3 Month	

Process Output:

S. No.	Outputs	To	Reference
a.	Information Security Management System Improvement Project Report	Concerned Dept.	
b.	Action Plans for Information Security Management System Improvements	-do-	

Process Monitoring:

S. No.	Monitoring Brief	Responsibility	Frequency	Reference
a.	Continual Improvement Project Status	MR	3 Month	
b.	Benefit Status of Completed Project	Concerned Head	After Completion	

8. Benefits

- Increase return on Information Security -related investments.
- Assist you in your pursuit of ambitious goals to get results that stick. Help boost productivity and overall business performance.
- Map the Information Security management plan directly to government requirements and mandates.
- Support response to shareholder inquiries.
- Generate accurate savings metrics to support communication

9. Exclusions

No waivers from this Policy will be accepted.

10. Records

- Information Security Management Plans (ISMPs)
- Annual Information Security Improvement Plan(ISIPs)
- ISMS Objectives and Metrics based on ISO 27001: 2013
- Master List Of All Monitoring And Measuring Requirements
- Monitoring And Measurement Report
- Action Plans for Improvements