INFORMATION SECURITY RISK MANAGEMENT POLICY

Cogent E Services Private Limited

Corporate Information Security Guidelines

COGENT E SERVICES PRIVATE LTD.

C 100, Sector 63,
Noida GautamBudh Nagar
Uttar Pradesh 201301,
INDIA .

www.cogenteservices.com

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

SECTION-I DOCUMENT DETAILS

DOCUMENT INFORMATION

Preface

The Cogent E Services Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent E Services 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.

VERSION CONTROL PROCEDURE

Draft Version: Any version of this document before it is finalized by all stakeholders i.e., process owners, client and ISO internal auditors, would be treated as 'Draft Version'.

The control number for the draft version would always start from '0'. For example first draft will have the control number as 0.1.

Final Version: Once the document is finalized by all stakeholders i.e., process owners, client and ISO Internal Auditor, it will cease to be a 'draft' and will be treated as 'final version'.

To distinguish between draft version and final version, the control number for finalized document would always start from an integer, greater than zero. For example, first final version will have the control number as 1.0.

Document Creation and Maintenance: This document would generally be written for the first time at the time of transition to ISO/IEC 27001:2013. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis. The Information Security Steering Committee (ISSC) members are responsible for approving any necessary amendments to the Cogent E Services Information Security Policy Documents. Changes to the Cogent E Services, ISMS Policy and ISMS Objectives shall be reviewed by the CISO and approved by Cogent E Services Information Security Steering Committee

Implementation Date: Implementation date is the date when the document is released and made operational in the ISMS. By logic, it should be after the approval date. All dates should be updated in MM/DD/YYYY format.

Amendment Procedure: The Cogent E Services Information Security Policy Documents shall be amended to reflect any changes to Cogent E Services capability or the Information Security Management System.

Summary of Changes: Version history table below denotes the nature and context of any update or change made in this document.

VERSION 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	

DISTRIBUTION AND CONTROL

Document Distribution

The Cogent E Services Chief Information Security Officer (CISO) shall distribute this document to all document change reviewer when it is first created and as changes or updates are made. The CISO shall distribute the document to members of Information Security Steering Committee (hereinafter referred to as ISSC) and Information Security Working Group (hereinafter referred to as ISWG).

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

One set of hard copies will be available with the CISO as controlled copy. All other soft and hard copies of the ISMS documents are deemed to be uncontrolled. The CISO will ensure that any update to the ISMS is incorporated on the intranet server and is communicated to all employees of Cogent E Services through an appropriate mode such as e-mail.

Distribution List

Name	Title
Information Security Steering Committee	ISSC
Information Security Working Group	ISWG
Chief Information Security Officer	CISO

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.

SECTION-II INFORMATION RISK MANAGEMENT POLICY

Cogent E Services Private Ltd. (Cogent E Services) has adopted ISO 27001:2013 , the International Standard for Information Security Management. The basic definition of Information Security in the context of the standard is "**The protection of the Confidentiality, Integrity and Availability of the Information Assets."**

This document will help in understanding the methodology to be used for identification and valuation of information assets and risk assessment adopted by Cogent E Services and thereby helps in the creation and maintenance of the **Asset Register and Risk Assessment** document for the respective Functions.

By following the guidelines functions will be able to perform a risk assessment such that it will result in:

- Identification of Information Assets
- The valuation of the asset in terms of its Confidentiality, Integrity and Availability (CIA) criteria
- Help in identifying the possible Threats and Vulnerabilities associated with the respective assets
- Arriving at the Risk rating for the respective assets and the selection of safeguards / controls for mitigating the risks.

Definitions

The key definitions are presented in this section. Unless specified these generic terms apply across the entire manual.

Asset:	Something that has value to the organization and is used for the business operations.

Information Asset:	Information asset is a body of information that the organization must have to conduct its business operations. For the purpose of this methodology, the information assets include the following types: hardware, software, business application, people, document and information (usually in electronic form). To differentiate in this methodology, information asset refers to all stated types. However, information asset (i) refers specifically to the type information.
Threat:	An incident or an unplanned event which can accidentally trigger or intentionally exploit a specific or multiple vulnerability(s) and have an undesirable effect on the well-being of an information asset.
Vulnerability:	The absence of or a weakness in the procedure, design, implementation or internal control of an information asset that can be accidentally triggered or intentionally exploited to disrupt the normal function of the information asset.
Owner:	The person responsible and accountable for the security of an information asset is the Owner. The owner determines the security requirements based on the risk assessment or contractual requirements and ensures that appropriate controls based on business requirements (which are commensurate to the assets classification and valuation) are implemented to reduce the likelihood of loss of Confidentiality, Integrity and Availability. E.g.: Group heads for Group related assets, Data Centre Head for common assets across Data Centre, Function heads for respective functions assets

Custodian:	The person responsible for securing the information assets as per requirements of the asset owner is the custodian. The custodian is the person responsible for the implementation & maintenance of the appropriate controls required for the security of the information assets. E.g.: Group Head / Admin as may be the case, DBA: Team server or any other corporate database administrators Admin: Firefighting, Access control systems, physical access to restricted area, Power supply, UPS, Precision AC
User:	User is a person who uses the information asset in compliance with the security policy of the organization to execute his tasks. Users must take "due care" to preserve the security of the information asset. E.g. Individual Desktop User / Application End User
Risk:	The net result of the adverse impact caused by the likelihood of a risk occurrence. The risk occurs when a threat(s) exploits a vulnerability(s) of an information asset.
Control:	Countermeasure or safeguard such as a procedure, action or mean that mitigates
	the undesired impact when an asset's vulnerability is exploited. One countermeasure may mitigate more than one risk.
Implemented Control:	An existing control in Cogent E Services 's environment.

Additional Control:	A control that does not exist in Cogent E Services 's environment, but is considered to be implemented to mitigate the risks. The need for implementing Additional Controls is decided during the Risk Mitigation and Treatment process.
Associated Control:	A control which work in cohesion with another control to mitigate a risk; Thus the net effectiveness of the controls is equivalent to the sum of the individual controls effectiveness.
Control Asset	A control that is exposed by its nature to risks; and thus is also treated like an information asset.
Risk Management:	The coordinated continuous processes of risk identification, assessment, mitigation, treatment and monitoring, to manage the risk which could potentially inhibit and tackle the organization from achieving its business objectives.
Risk Identification:	The process of identifying the risks based on incidents of risk occurrence, or an intentional effort of threats and vulnerabilities identification in relation to Cogent E Services 's information assets.
Risk Assessment:	The overall process of analyzing and evaluating the risk. When the controls are not considered in the assessment, it is the inherent risk that is evaluated. Whereas when controls are considered in the assessment -part of the mitigation process- then it is the residual risk that is evaluated. *Risk Assessment = Risk Analysis + Risk Evaluation*
Risk Analysis:	The systematic method to evaluate the risk impact -by rating the threat and vulnerability- and to estimate the risk likelihood.

Risk Evaluation:	The process of comparing the estimated risk impact and likelihood against given criteria –an impact vs. likelihood matrix, or quantitative bands- to evaluate and determine the level (significance) of the risk.
Inherent Risk:	The risk level for an information asset without considering the implemented controls.
Risk Mitigation:	The process of identifying the most appropriate control or set of controls to manage the risk by evaluating the controls cost, effectiveness and using cost benefit analysis to selecting the most appropriate control, evaluating the final residual risk and deciding on the risk mitigating option.
Intermediate Residual Risk:	The remaining risk of an information asset after considering the effectiveness and efficiency of implemented controls.
Final Residual Risk:	The remaining risk of an information asset after considering the effectiveness of additional controls.
Risk Acceptance:	A risk mitigation option where the decision is made to accept the risk.
Risk Avoidance:	A risk mitigation option where the decision is made to withdraw from- or not become involved in- the risk circumstance and situation.
Risk Reduction:	A risk mitigation option where the decision is made to reduce the adverse impact of the risk by implementing appropriate countermeasures.
Risk Transfer:	A risk mitigation option where the decision is made to share with another party insurance- the burden of loss in the event of a risk occurrence.

Risk Treatment:	The process of implementing the risk reduction options that comprises a list of the selected additional controls.
Risk Monitoring:	The process of monitoring the implementation of the risk treatment plan and triggering risk reassessments as required ensuring the continuity of the risk management process.

.

Introduction

Background

Information Risk Management (IRM) is the systematic method of establishing the context of, identifying, analyzing, evaluating, treating, monitoring, and communicating risks associated with any activity, function, or process of an information asset, in a way that will enable the Central Authority for Information Technology (Cogent E Services) to minimize losses.

Purpose

The main purpose of Information Risk Management is to make a judicial use of the resources at the disposal of Cogent E Services and provide the best possible protection to its information assets at an appropriate cost. The IRM methodology provides practical guidance required for identifying assessing, mitigating and monitoring risks associated with information assets.

Scope

The scope of the IRM methodology applied to all information assets and the underlying technology infrastructure, related processes and human resources involved in managing the IT environment. The IRM methodology is intended to be used by the information security function of Cogent E Services.

Target Audience

The IRM methodology enables IS Department to make informed decisions to justify IT costs and budgets for implementing the mitigation and treatment plans that aim to minimize the impact of the residual risks to an acceptable level.

The output of the IRM processes assists the ITs, Information Security professionals at Cogent E Services to obtain an insight into information assets risks for improving the internal and overall security controls within the organization. This improvement of the

information security can then contribute to Cogent E Services competitiveness in the industry by demonstrating the organization efforts to stakeholders and customers.

Overall, the IRM methodology provides an assurance to the Senior Management that the risks within the Cogent E Services ISMS related to people, process and technology are proactively managed in a cost effective manner.

Structure of the Document

Section one is an introduction section to explain the purpose, scope and target audience of the IRM methodology.

Section two provides an overview of the IRM methodology, explains the objective and benefits of risk management, outlines the key roles of Cogent E Services personnel to support and implement the IRM framework and sets the definitions of key terms.

The IRM methodology is described in the four remaining sections of this manual.

Section three describes the risk identification and reporting process. It discusses the different triggers and source information for this process and the elements required to start building a risk register

Section four describes the risk assessment process. It presents a detailed explanation of the formulas and criteria used for risk analysis and evaluation.

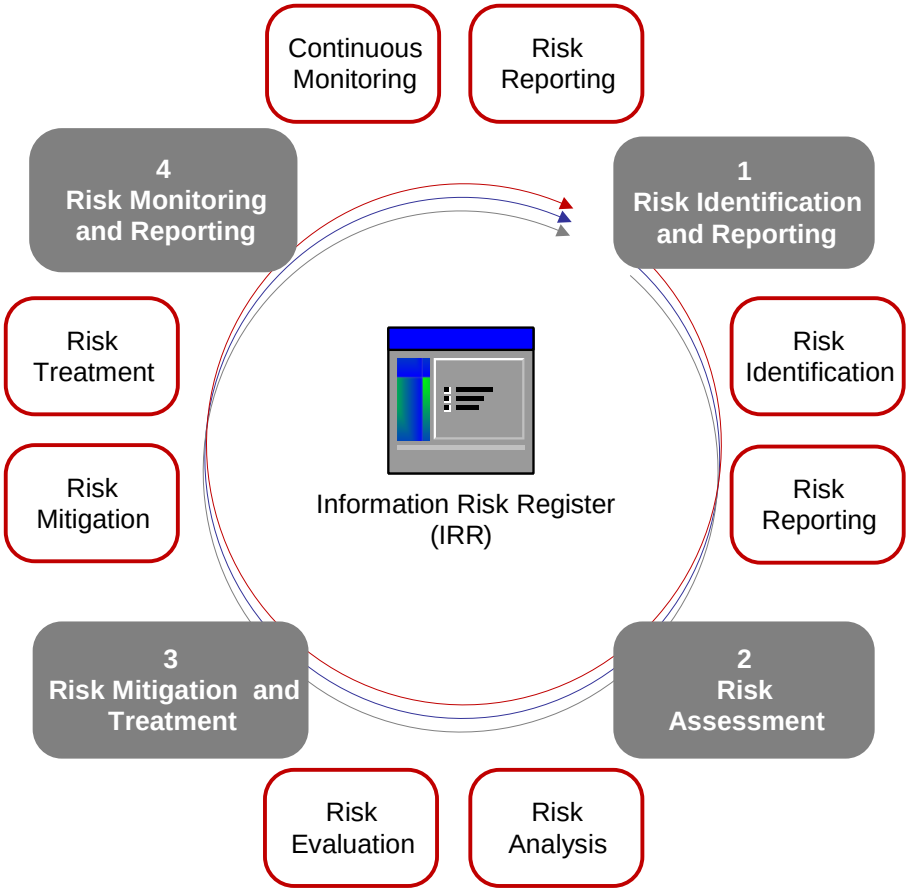
Section five describes the risk mitigation process to derive a residual risk based on existing controls, and additional controls. It details the steps for reassessing the risk with consideration of existing and additional controls. This section also describes the elements required to develop a risk treatment plan, and the rules for prioritizing implementation of new controls.

Alignment to IRM good practices

The techniques used in this IRM methodology are inferred from various leading IRM practices (such as Risk Management with ISO 31000:2009 –Principles and Guidelines on Implementation,
ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition) , OCTAVE, CRAMM). However, the methodology is customized to suit the specific requirements of Cogent E Services

Information Risk Management (IRM) Overview

IRM is a continuous cycle to minimize the negative impact of an unplanned event (risk) on information assets which would eventually impact the business operations.



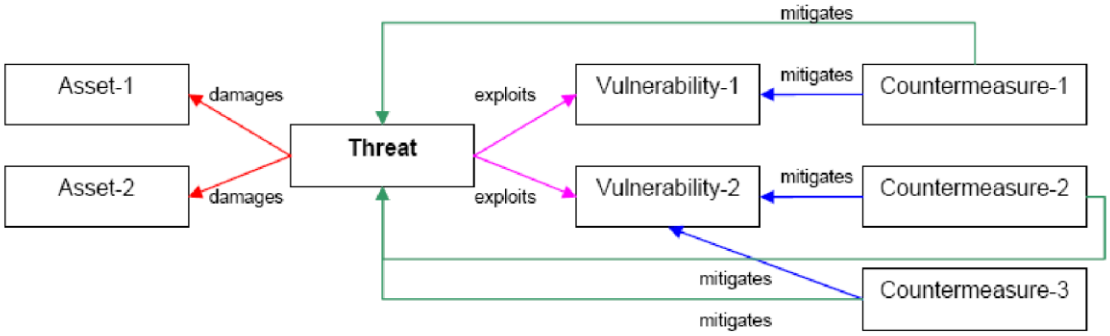
The IRM methodology comprises of the following four processes:

IRM Processes	Definition

Risk Identification & Reporting	Risk Identification is the process of identifying and reporting the events (incidents), and determining the existing threats and vulnerability occurrences that affected or may affect the information assets.
Risk Assessment	Risk Assessment is the process where all identified risks are analyzed and evaluated to determine the level of inherent risk. It involves assessing the risk elements -threat and vulnerability to determine the associated impact on the
IRM Processes	**Definition**
	information asset, and determining the risk likelihood to derive the inherent risk value.
Risk Mitigation and Treatment	Risk Mitigation and Treatment is the process of identifying possible controls that would assist in reducing the overall risk which an asset is exposed to. The identified controls are evaluated for their design and operating effectiveness. A cost benefit analysis is then performed to select suitable controls for implementation. In some cases where there are no controls to implement, or the costs outweighs the benefit, the risk may be accepted by the business.
Risk Monitoring and Reporting	Risk Monitoring and Reporting is the process whereby the risks impacting information asset is are evaluated on a regular basis. This is performed to identify changes in the threat and vulnerability profiles which may change the overall risk level of information assets. .

Communication and coordination is a key element in IRM. To ensure the success of IRM, it is vital that the result of each IRM sub process is communicated to the concerned parties within a reasonable time period. Coordination is also important, as the IRM program would involve number of people working in different departments or areas. A well-controlled communication and coordination mechanism between the various involved people is one of the critical success factors for an effective and efficient IRM program.

Elements of the IRM Methodology



The following elements are used in the IRM methodology:

- Asset
- Threat
- Vulnerability
- Control (Countermeasure)

Key Roles

IRM is a joint responsibility of senior management, IT management, business management, security specialists, IT support specialists and information asset owners. This section provides an overview of the key roles involved in the IRM methodology.

Information Security Steering Committee (ISSC)

- Oversee the management and implementation of the Information Risk Management Process
- Review and approve on the overall information security risk exposure to Cogent E Services
- Review the IRM program outputs; and
- Ensure that the decision-making for IT planning and budgeting considers the output of the IRM program.

Board of Directors:

- Allocate the necessary resources for effective implementation of the IRM program in order to mitigate the information risks that can potentially inhibit the achievement of the business goals; and

- Balancing the trade-offs for controls implementation to ensure that the business goals are achieved effectively with minimal expenditure of resources.

Information Security Manager:

- Undertake periodic risk assessments based on a schedule or as per organizational requirements; and
- Publicize IRM awareness among the organization's employees to effectively contribute to the IRM process.

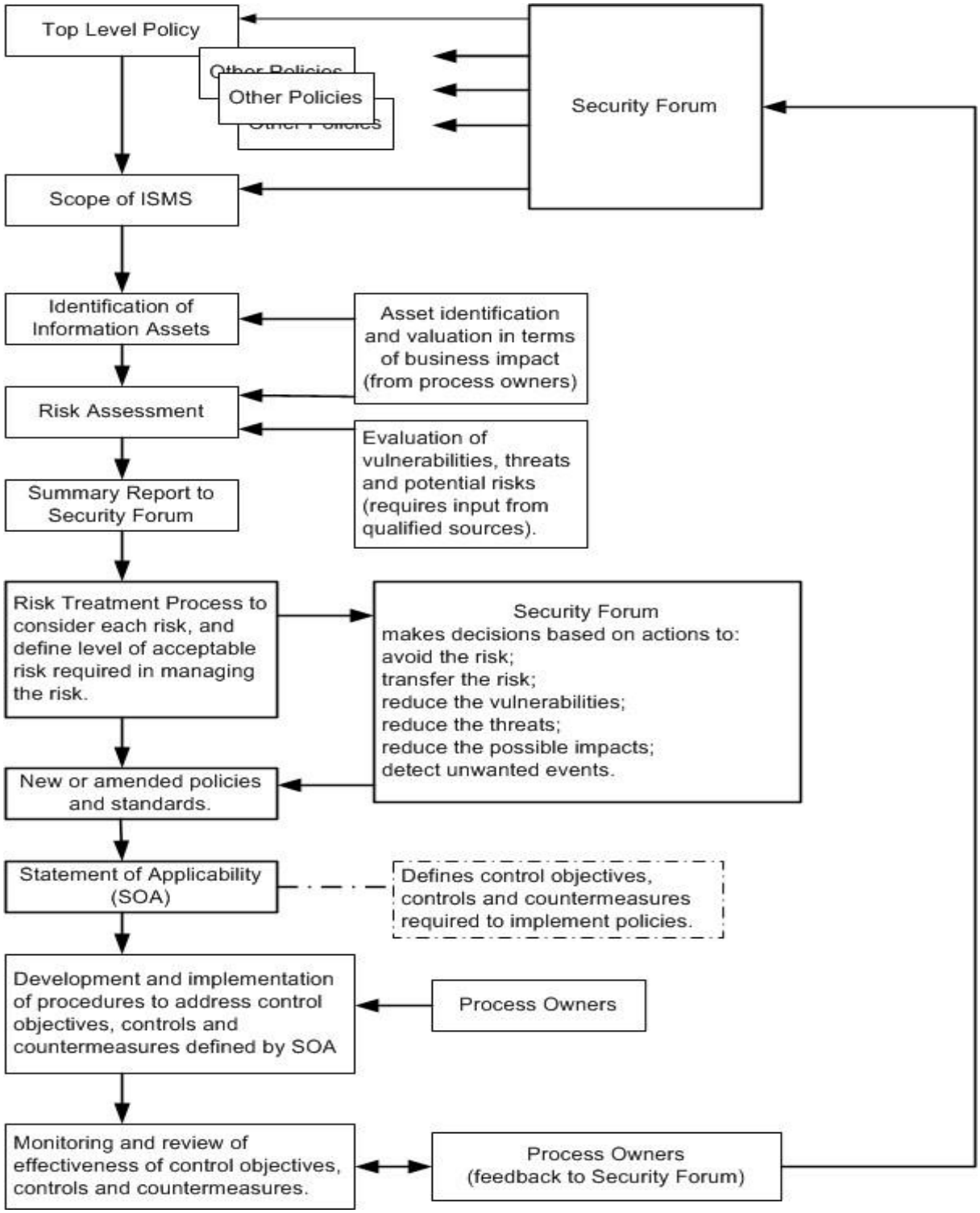
Information Risk / Asset Owners:

- Ensure that sufficient and effective controls are in place to address the confidentiality, integrity and availability of the systems and information assets they own.

Risk Assessment Methodology

The Risk assessment methodology adopted by the organization is a step-wise process that starts with the identification of information assets and culminates with the identification of controls that need to be implemented to mitigate the risks identified.

The Information Asset Register template is used for creating and maintaining the Information Asset Register for the respective Functions. Once the asset identification process is completed the accompanying Risk Assessment Methodology document is used to arrive at the valuation and risk rating of the asset.



Identification of Assets

This phase deals with identification, listing and valuation of all information assets for the Cogent E Services / Project / Function. The following categories of assets are included in the asset register.

Information Asset - This would include Databases & Data files (including important data in local desktops/laptops), System documentation, User documentation, Training materials, Operational / Support procedures, Continuity plans, Archived information etc.

Information Asset can be further sub-categorized into two formats - Electronic (or) Hard Copy.

Software Asset - This would include Application software, System software, Development tools & Utilities etc.

Hardware/Physical Asset - This would include Computer equipment (processors, monitors, laptops, modems, printers etc.), Communication equipment (Network devices, EPABX, Fax machines etc.), Unused magnetic media (Tapes, Disks, CDs) etc.

Services - This would include general utility services such as Power, Lighting, and Air Conditioning, Communication links, housekeeping services, security services, background verification services, recruitment services, facility management services, etc.

People - This would include personnel required to support and run other assets.

Asset classification and valuation

Having identified and listed all the assets in the Asset register, the next step is the classification of the assets into various assets classes defined .

The asset Classes are then rated on the basis of the **C**onfidentiality, **I**ntegrity and **A**vailability rating based on the methodology adopted. This is done by evaluating the asset classes with respect to impact it will have due to unauthorized disclosure, loss of integrity due to unauthorized modification or damage and un-availability of the asset when required in a scale of 1 –3 as per the methodology mentioned below:

Confidentiality Rating

Rating	Definition	Examples
3	These information / assets are restricted to Management and are intended for business use. Impact of unauthorized disclosure can result in: • Severe disruption in business operations of the company or part of the company • Adverse publicity • Law suits and/or • Significant business loss / financial loss The classification of such information is **Restricted, Top secret, Limited, Concealed, Proprietary**	1. Financial and other company related information required to be informed to the stock exchanges under the listing agreement prior to release 2. Draft policy documents under formulation 3. Employee remuneration / compensation related information 4. Customer provided information requiring confidentiality as per request or classification, etc.
2	These information / assets are permitted to be shared / used within a group of users / team for the purpose of the project / function. Impact of unauthorized disclosure can result in: • Affecting the functioning of the individual projects / functions. • Adverse impact on relations with customers and business associates. • Adverse effect on employees • Minimal business / financial loss	Memos, Work programs, Schedules, Test results, Status reports, Software code, Project plans and other project related artifacts, TEAMS application and content, Software Requirement Specifications, User mailbox access

	Classification of such information is **Sensitive**, **Secret, Confidential, Private, Strictly Personal and Confidential**	
1	These information / assets are permitted to be shared / used by all the employees (authorized users) of the company. Unauthorized disclosure outside the company is against policy. Disclosure however, is not expected to seriously impact the company, employees, business partners, customers and /or other stakeholders.	Training material, Policy manuals, QMS documents and templates, ISMS documents and templates, Other policies and resources available on the website and intranet, company policies and schemes, SOP
	Classification of such information is **Internal, Company internal**	
1	These information / assets have been explicitly approved by management for release in the public domain and may be shared freely with all including outsiders (unauthorized users) without any potential harm.	Information available on the Cogent E Services website, sales brochures and pamphlets, press releases
	Classification of such information is **Public**	

Integrity Rating

Rating	Definition

3	Loss of integrity of the information / asset (either partially or completely) could lead to: Significant Business, Financial and / or Legal Impact Embarrassment and / or negative publicity to the company The integrity of the information in this case either cannot be recovered or may be totally or partially recoverable at a significant and material financial cost.
2	Loss of integrity of the information / asset (either partially or completely) would lead to: A business impact for a project / function. The information can be recovered (either partially or completely) with some level of effort and minimal financial cost.
1	Loss of integrity of the information / asset would moderately affect the completeness of the information and low business impact. The information can be recovered with minimal effort.
1	No impact due to loss of integrity of the information / asset.

Availability Rating

Rating	Definition
3	The information / asset is such that: Non-Accessibility or Unavailability would constitute disruption in work leading to high impact to the business operations and / or financial loss to the company. Replacement is possible at a very high cost, effort and will require a lot of time to restore Tolerance to unavailability is very low Loss due to unavailability is very high Required for legal and regulatory compliance This would typically apply to assets where Maximum Permissible Downtime is 4 hours or less. E.g.: Mail Server, Contingency Assets, Link Failure, Internet connection etc.
2	The information / asset is such that: Non-Accessibility or Unavailability would constitute a disruption in work leading to business impact to a part of the company Replacement is possible at a high cost and will require a lot of effort and time to restore This would typically apply to assets where Maximum Permissible Downtime is 1 working day or less.

1	The information / asset is such that: Non-Accessibility or unavailability would constitute a disruption of work leading to impact on the functioning of individual projects / functions Loss due to unavailability is moderate, provided functions are restored within a certain timeframe Non-availability of asset may have some impact on Cogent E Services , if prolonged for a long period of time. For example, assets where Maximum Permissible Downtime is between 1 & 5 working days
1	The information / asset is such that: Non-Accessibility or Unavailability would constitute a disruption in work leading to low or no business loss. Asset can be easily replaced These assets may be unavailable for an extended period of time, at little or no cost to the company, and require little or no effort when restored. Non-availability of asset would have minimal / insignificant impact on Cogent E Services . For example, assets with Maximum Permissible Downtime greater than 5 working days

Once the classification of the assets based on the ratings given for the C I A criteria is done the asset value is computed as follows:

Asset Class Value = Confidentiality + Integrity + Availability

Below is the matrix to be used for Risk Management

Asset Value Index	Classification	Risk Management Actions
3	**Critical:** Confidentiality + Integrity + Availability is 8-9	Mitigation on high priority
2	**Important:** Confidentiality + Integrity + Availability is 6 – 7	Mitigation plan is required
1	**Moderate:** Confidentiality + Integrity + Availability is 3-5	Should be monitored and reviewed regularly
0	**Low:** Confidentiality + Integrity + Availability is < 3	No specific action required however, may require to be tracked at the time of reviews

Based on the C I A rating of the individual asset classes the Asset value index shall be computed as per the above table, the asset value index ranging from 1 to 3. However, in the case of the following exceptions a significantly higher asset value index may be assigned:

1. In the cases when a specific legal, regulatory or contractual compliance is required in a project or function the appropriate information assets shall be assigned a higher asset value so that it necessitates the implementation of adequate controls and safeguards to ensure compliance.

2. In the case when any one of the C I A rating value is the highest (3) the asset will be treated as a very critical asset for ensuring that mitigation plans / adequate safeguards have been implemented.

3. Use of messenger applications, web browsing and web mail access iis governed by the acceptable use policy in force. The use of these applications provides an opportunity for virus infections and can also be a source for information leakage.

   Based on the C I A criteria adopted it is likely that the asset value will appear to be low for these applications. Hence, in the absence of any technical safeguards for controlling information leakage and or virus attacks, based on the sensitivity of the information available to an individual having these applications installed a higher asset value shall be assigned to the Asset value to ensure that the risk rating is always greater than 1. Such cases will be taken up at the IMS Forum for acceptance of risks.

Overall Asset Classification Rating

Public – This classification applies to information, which has been explicitly approved by Cogent E Services management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. Data integrity is not vital & non-availability is an acceptable risk. E.g. Information generated for public consumption such as public bulletins, marketing flyers etc.

Internal – Data whose unauthorized disclosure is against policy but it is not expected to seriously or adversely impact Cogent E Services its employees / customers stockholders & business partners. E.g.: Cogent E Services telephone directory, training materials, and policy manuals

Confidential – This classification applies to less sensitive business information, which is intended for use within Cogent E Services . Unauthorised external / internal access to the asset would impact Cogent E Services and/or its partners/customers. Access should be restricted. e.g.: Customer information, Personnel records, critical operational information

Restricted/Secret – This classification applies to the most sensitive business information, which is intended strictly for use within Cogent E Services . Its unauthorized disclosure could seriously and adversely impact Cogent E Services , its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion. The asset is of strategic importance to Cogent E Services , criticality is highest, and the asset needs the highest level of protection. e.g.: Merger and acquisition plans, Business plans planning for existing litigation, trade secrets, customer data, information security data, Strategy Documents etc.

- Access privileges to the files and folders have been granted appropriately by the VPIT/ AM/ Team Lead, as per the data classification.
- Hard copies also need to be stored separately for each project under appropriate facilities provided for under each classification.

- All hard copies need to be appropriately labeled as per their classification. This can be in the form of either a stamp on the document itself or a label on the cupboard/ drawer on which it is stored.

Identify Threats and Vulnerabilities

THREAT

A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Natural threats, accidental threats, human accidental threats, and human malicious threats are included. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism.

Each potential Threat is assigned a Impact value as per table given below ranging from 1(Low) – 3(High)

Impact Value of Threats for each Asset Class

1	**Low**
2	**Medium**
3	**High**

The Following Threats have been considered as Significant for Cogent E Services and the impact ratings on various Information Asset Classes are given as under :

Sl No	Threat	Impact
1	Theft and Fraud	**2**
2	Hacker/Crackers (Internal/ External)	**3**
3	Malicious Acts(Virus, Worms, Trojan Horses)	**3**
4	Unauthorized Access /Change	**2**

5	Operator Error	**2**
6	Effecting on Reputation	**3**
7	Off Premise Security	**2**
8	Software/Application Malfunction /Failure	**2**
9	Environment (Temperature/ Humidity/Water)	**2**
10	Power Loss/Fluctuation	**3**
11	Equipment Malfunction	**2**
12	Equipment Failure	**3**
13	Lawsuits and Litigations	**3**
14	Data Loss/Corruption	**3**
15	Civil Disorder/Vandalism (Riot, Arson)	**2**
16	Willful Damage	**3**
17	Attrition/Loss of Life /Staff Shortage	**2**
18	Asset/Resource Misuse	**2**
19	Terrorist and Bomb related attacks/ threats	**3**
20	Natural Disaster (earthquake, flood, Strom, Cyclones etc)	**3**
21	Unavailability of Facilities (Buliding, Network, Server)	**3**
22	Fire	**3**

VULNERABILITY

Vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.

Each potential Vulnerability is assigned a Probability value as per table given below ranging from 1(Low) – 3(High)

Probability Value	
1	Low
2	Medium
3	High

The Following Vulnerabilities have been considered as Significant for Cogent E Services and the probability ratings on various Information Asset Classes are given as under

Sl. No.	Vulnerabilities	Probability
1	Improper Physical Access Controls	2

2	Improper Logical Access Controls	2
3	Improper control /Approval Procedure for addition/ movement of assets	3
4	Inadequate asset management (accountability of software/hardware)	3
5	No network/ system security & control	2
6	No Malicious activity prevention and detection mechanism	2
7	Improper change management	2
8	Unwanted port/ services enabled	2
9	Week Passwords & default configuration/accounts enabled	2

Sl. No.	**Vulnerabilities**	**Probability**

10	Lack of user identification/authentication mechanism	2
11	Communicating/Publishing Additional/Irrelevant Information	2
12	No Security awareness training (Improper Awareness /Mock Drills on handeling security incidents (Fire, naturial))	2
13	No incident management process	3
14	No control of Mail/ Browsing/IM	3
15	No security in electronic commerce services	0
16	Lack of Log Maintenance and Monitoring	3
17	Lack of testing and installing procedures (Patches, Anti Virus, Software, Application)	2
18	Improper configuration of Devices, services and applications	2
19	Poor/Lack of Documentation	3

20	Lack of capacity planning	3
21	Inadequate backup procedures (Retentions, Labeling, Storage and testing plans)	2

Sl. No.	Vulnerabilities	Probability
22	Complicated user Interface	2
23	Violation of Legal/Statutory/Contractual Provisions	3
24	Inadequate information security policy/ Business long-drawn-outage (BCP/DR)	3
25	Inadequate control over Third Party Vendors, Contractors, Customer	2
26	Inadequate Knowledge transfer	2
27	Inadequate Monitoring and Mainantance of Devices / Equipment (AC, UPS, DG, Servers, Network & Security Devices)	2
28	Inadequate power backup devices (DG, UPS)	1

29	Failure of redundant equipment	1
30	Insecure handeling of equipment	2
31	Inadequate review of contracts and Agreements	1
32	Network/ Power/ Telecom Cable Failure	3
33	Improper data processing in applications	2
34	Inadequate contacts with local authorities (Police,	2
Sl. No.	**Vulnerabilities**	**Probability**
	Fire, Ambulance)	
35	Absconded/ disgruntled employee	2
36	Lack of HR policies	2
37	Lack of segregation of duties	2
38	Lack of Safety measures on physical infrastructure	2
39	No/malfunctioning of Fire Alerting/ Protection Mechanisms / Fire Exits	3

40	Inadequate monitoring of external parties	2
41	Inadequate monitoring & review of security management systems	3

Risk Assessment

For each threat/vulnerability pair, the severity of impact upon the system's confidentiality, integrity, and availability is determined, and the likelihood of the vulnerability exploit occurring giving existing security controls is also determined.

The product of the likelihood of occurrence and the impact severity for each asset class is done and the results in the risk level for the asset class based on the exposure to the threat/vulnerability pair.

Once the risk level is determined for each threat/vulnerability pair, safeguards are identified for pairs with moderate or high risk levels.

The risk is re-evaluated to determine the remaining risk, or residual risk level, after the recommended safeguard is implemented.

Impact Rating =

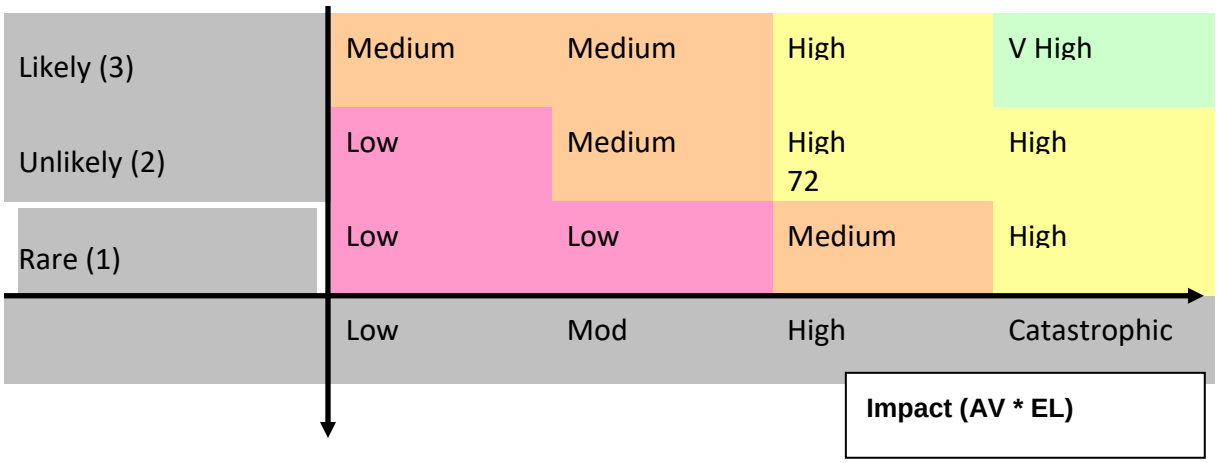
Impact Value of Threats for each Asset Class

1	Low
2	Medium
3	High

Probability /Likelihood

Likelihood: The probability of potential vulnerability may be exploited with associated threat and environment	
3	**Likely:** The controls to prevent vulnerability exploitation are in place (exists) however may impede successful exploit. Threat source is motivated
2	**Unlikely:** The controls to prevent vulnerability exploitation are in place (exists) however may significantly impede successful exploit. Threat source lacks motivation
1	**Rare:** The controls to prevent vulnerability exploitation are highly effective and detective in nature.

Risk Value = Likelihood X Impact



Risk Priority Number

4	Very High	Immediate Action along with the involvement of Management
3	High	Management directives should be specified along with timelines
2	Medium	Managed by proactive monitoring
1	Low	Managed by routine process

Describe Risk

Describe how the vulnerability creates a risk in the system in terms of confidentiality, integrity and/or availability elements that may result in a compromise of the system and the data it handles.

Identify existing controls

Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

RATING CONTROLS

Each control selected for a threat in the earlier step is now being evaluated, to ensure its performance and effectiveness in mitigating/reducing the threat to the asset.

The effectiveness of control is rated in a scale of 1 to 4, 1 being minimum and 4 being highest. The rating of controls is done based on data captured as part of the ISO 27001 :2013 initiative in gap analysis, vulnerability assessments, operating systems review, database review, network reviews, etc.

In Gap analysis, all the 133 control points were rated on the scale on 1-4 with respect to the present implemented controls. (1 indicates no control implemented and 4 indicate the control implemented is appropriate.)

Calculating Existing Residual risk

In this step, the existing residual risk is determined. The existing residual risk is the risk faced by the organisation after instigating the controls, which are operational

The existing residual risk is computed by subtracting the control rating from the Expected loss value of an asset, i.e.

Existing Residual Risk = ELV of asset – Control Rating

The control rating defined is derived from the above section.

The possible values of existing residual risk are:

1st Slab:	1	No residual risk
2nd Slab:	2	Low Residual risk
3rd Slab:	3	Moderate Residual risk
4th Slab:	4	High Residual risk
5th Slab:	5	Very High Residual risk

The organisation has to decide whether accept the risk (take no action), reduce the risk (by instigating new controls or strengthening existing controls) or transfer the risk (insure the assets).

The assets for which the residual risk is low, moderate, high or very high for a particular threat, risk mitigation plan or risk treatment plan is advised to be applied in order to reduce further the residual risk.

Identify Safeguards / Mitigation Plan

Having identified the risk priority the completed assessments are reviewed. If the Risk priority is 1 the risk can be accepted by the assessment team of the Group / Function.

The following categories of safeguards may be selected depending on the specific requirements applicable to the asset.

- Accept
- Avoid
- Reduce & control
- Transfer

For cases where the Risk priority is greater than 1 planned control need to be identified and implemented. This process may involve the need to consult with other support groups to help identify appropriate controls that can be applied. Once a control is planned a plan needs to be prepared to ensure its implementation.

There may be some cases when a planned control that can be implemented may have a financial implication and budgets may be necessary, all such cases will require to be escalated up to the Delivery Head / Location Head for the respective Groups & Functions and to the Resource Head for cases that require company – wide implementation. Risks associated for such cases till such time that the safeguard has been implemented shall have to be accepted at the Management level.

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination Phase.

The purpose of the recommended safeguard is to reduce or minimize the level of risk. When identifying a safeguard, consider the:

(1) Security area where the control/safeguard belongs, such as management, operational, technical;

(2) Method the control/safeguard employs to reduce the opportunity for the threat to exploit the vulnerability;

(3) Effectiveness of the proposed control/safeguard to mitigate the risk level; and

(4) Policy and architectural parameters required for implementation in the Cogent E Services environment.

Recommended safeguards will address the security category identified during the risk analysis process (confidentiality, integrity and availability) that may be compromised by the exploited vulnerability.

If more than one safeguard is identified for the same threat/vulnerability pair, list them in this column in separate rows and continue with the analysis steps: the residual risk level must be evaluated during this phase of the assessment and may be further evaluated in risk management activities outside of the scope of this methodology.

If a complete implementation of the recommended safeguard cannot be achieved in the Cogent E Services environment due to management, operational or technical constraints, annotate the circumstances in this space and continue with the analysis.

Risk Assessment Report

The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

Risk Treatment Approach

Risk Mitigation Plan

Also referred to as Risk Treatment Plan. A mitigation plan is prepared for each threat where residual risk exists.

Having identified the risk priority the completed assessments are reviewed. If the Risk priority is 1 the risk can be accepted by the assessment team of the Group / Function.

The following categories of safeguards may be selected depending on the specific requirements applicable to the asset.

- Accept
- Avoid
- Reduce & control
- Transfer

For cases where the Risk priority is greater than 1 planned control need to be identified and implemented. This process may involve the need to consult with other support groups to help identify appropriate controls that can be applied. Once a control is planned a plan needs to be prepared to ensure its implementation.

There may be some cases when a planned control that can be implemented may have a financial implication and budgets may be necessary, all such cases will require to be escalated up to the Delivery Head / Location Head for the respective Groups & Functions and to the Resource Head for cases that require company – wide implementation. Risks associated for such cases till such time that the safeguard has been implemented shall have to be accepted at the Management level.

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination Phase.

The purpose of the recommended safeguard is to reduce or minimize the level of risk. When identifying a safeguard, consider the:

(1) Security area where the control/safeguard belongs, such as management, operational, technical;

(2) Method the control/safeguard employs to reduce the opportunity for the threat to exploit the vulnerability;

(3) Effectiveness of the proposed control/safeguard to mitigate the risk level; and

(4) Policy and architectural parameters required for implementation in the CMS environment. Recommended safeguards will address the security category identified during the risk analysis process (confidentiality, integrity and availability) that may be compromised by the exploited vulnerability.

If more than one safeguard is identified for the same threat/vulnerability pair, list them in this column in separate rows and continue with the analysis steps: the residual risk level must be evaluated during this phase of the assessment and may be further evaluated in risk management activities outside of the scope of this methodology. If a complete implementation of the recommended safeguard cannot be achieved in the Cogent E Services environment due to management, operational or technical constraints, annotate the circumstances in this space and continue with the analysis.

The Mitigation plan elaborates the actions to be taken in order to reduce the residual risk of the asset to acceptable levels. Cogent E Services should plan for risk mitigation, i.e. reduce or accept the risk where the residual risk of the asset is equal to or greater than “Moderate”. For cases where residual risk is “Low” or “Negligible”, Cogent E Services would accept the risk.

The mitigation plan is prioritized based on residual risk i.e. where residual risk is "Very High", controls relating to same should be implemented first, followed by controls relating to "High" residual risk and then controls relating to "Moderate" residual risk

The mitigation plan will briefly explain the action to be taken and may draw reference to other issued reports

e.g. Gap Analysis Report, Vulnerability Assessment Report, Application Review Report, etc.

Responsibility and target date

The person from the organisation who will be responsible in implementing the controls is mentioned in the risk mitigation plan and the expected target date for completely implementing such controls.

Risk Acceptance Criteria

Risk acceptance is the decision of the management to accept a risk. Management decision is taken after considering the existing residual risk and the mitigation plan. Management, factors in the following aspects with regard to accepting the risk and / or implementing the control will:

- Require investments (both in people resources and money),
- Require time of implementing the control, and Possibly be complex or difficult to implement.

The management then approves the residual risk and authorises the implementation of controls. In cases, where management decides to accept the existing residual risk i.e. authorization is not granted for implementation of controls, the reasons for the same are recorded.

4.0 Appendix 1 – Legend Overall Asset Classification Scheme for Cogent E Services

PUBLIC	This classification applies to information, which has been explicitly approved by Cogent E Services management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.
INTERNAL	This classification applies to all other information, which does not clearly fit into any of the other three classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact Cogent E Services its employees / customers stockholders & business partners.
CONFIDENTIAL	This classification applies to *less sensitive* business information, which is intended for use within Cogent E Services . Its unauthorized disclosure could adversely impact Cogent E Services , its stockholders, its business partners, its employees, and/or its customers. Information that some people would consider to be private is included in this classification.
RESTRICTED /SECRET	This classification also applies to the most sensitive business information, which is intended strictly for use within Cogent E Services . Its unauthorized disclosure could adversely impact Cogent E Services , its stockholders, its business partners, and/or its customers leading to legal and financial repercussions and adverse public opinion.

The exception to the above computation would be in cases where there is no rating for confidentiality and integrity (such as hardware assets – where availability is the only rating). In such cases, the rating of availability is extrapolated.

Enforcement

1. Any infractions of this code of ethics will not be tolerated and Cogent E Services will act quickly in correcting the issue if the ethical code is broken.

2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

END OF DOCUMENT