SECURITIES & EXCHANGE BOARD OF INDIA

Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification

EXPRESSION OF INTEREST

SEBI/ITD/HO/2020/12/01

Contents

SECTION I – INTRODUCTION

1. Securities and Exchange Board of India (SEBI) is a statutory body, which operates within the legal framework of Securities and Exchange Board of India Act 1992. Its statutory objectives are:
    a. Protection of interests of investors in securities
    b. Promotion and development of the securities market
    c. Regulation and supervision of securities market and matters incidental thereto

2. SEBI invites Expression of Interest (EOI) from established, reputed and reliable Solution Providers (Bidders) for *"Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification"* and have necessary capability, suitable capacity and relevant experience to provide these services.

SECTION II – SCHEDULE OF EVENTS

SN	Event	Date
1.	Date of commencement of EOI Process	December 15, 2020
2.	Last date and time for receipt of queries (through emails only) for clarification from applicants	December 24, 2020 05:00 PM
3.	Last Date and Time for EOI Submission along with all supporting documents.	January 08, 2021 03:00 PM
4.	Opening of EOIs	January 08, 2021 04:00 PM

SECTION III – BACKGROUND

1. IT risk assessment helps to determine the vulnerabilities in information systems and the broader IT environment, assess the likelihood that a risky event will occur, and rank risks based on the risk estimate combined with the level of impact that it would cause if it occurs. It will also help in identifying controls and measures required to be included in IT policies and Standard Operating Procedures (SOP).

2. The concept of risk is a key consideration in policy making. A well written Organization level IT policy, procedure and manual reduces operating costs and improves performance by enhancing consistency and establishing clear criteria for computer, network, hardware, software, information security, and IT vendor management. Establishing consistent IT SOP best practices and operational methods are an important component in safeguarding information systems, IT assets, and IT investments.

3. SEBI intends to conduct risk assessment, prepare policy documents, standard operating procedures (SOPs), documentation of procedures and processes and other IT documents through consultation. SEBI also requires design specification document to be prepared for all the selected processes for automation.

4. SEBI has certain policy documents in place which might require variations as per the best industry standards and practices.

5. SEBI expects to prepare and implement a suitable governance structure i.e. comprehensive policy and procedure documents that are custom-made to suit to the needs of the business and advising staff of their obligations to ensure ongoing compliance.

6. Expression of Interest (EOI) is invited in sealed envelope superscripted as “EOI - *“Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification”:*
    1. from the Bidders who meet the eligibility criteria as set out in “SECTION V”
    2. agree to abide by all the other terms and conditions in this EOI document

    By participating in this bidding process Bidder confirms that bidder is in agreement with all the Terms and Conditions of this EOI.

SECTION IV – SCOPE OF WORK

The overall scope of work of the Bidder(s) would be as follows:

Following is the indicative list of activities envisaged to meet the scope of work. However, the detailed scope of work / list of activities would be finalized at the time of issue of RFP.

Risk Assessment

1. Bidder is required to perform in-depth Risk Assessment for IT infrastructure deployment at SEBI. The risk assessment needs to include identification of foreseeable threats, assessment of the likelihood and potential damage of these threats, and the sufficiency of controls to mitigate risks.

   The process should include but not limited to the following:
   - 1.1 Data classification categories
   - 1.2 Inventory systems
   - 1.3 Initial risk of each system
   - 1.4 Group Technologies
   - 1.5 Vulnerabilities and threats for each system
   - 1.6 Threat Assessment
   - 1.7 Controls for each vulnerability or threat
   - 1.8 Classification of controls
   - 1.9 Acceptable approach for Controls
   - 1.10 Residual Risk
   - 1.11 Reports

2. Bidder is supposed to conduct risk assessment of IT infrastructure deployment at SEBI annually, calculate risk score accordingly, review controls and its impact on Policies and SOPs and changes required in the reviewed policies and SOPs. Details regarding frequency and activity are mentioned in Section VIII Point 17.

3. Bidder is required to define risk assessment methodology for SEBI in order to define the rules by which risk assessment will be performed. The methodology needs to address following four issues:

   a. Baseline security criteria;
   b. Risk scale; categorizes risks along a multidimensional ranking, based on a comparative evaluation of the consequences, probability, and source of a given risk

c. Risk appetite; level of risk that SEBI is prepared to accept in pursuit of its objectives
d. Scenario-based or asset-based risk assessment.

Project wise as well as organizational level risk assessment methodology defined for SEBI shall be documented and shared with SEBI for approval. The methodology shall include following:

3.1 Identify and prioritize assets

SEBI maintains inventory list of all IT assets. Bidder is required to identify information assets of SEBI from the inventory list and other details available with SEBI. Bidder has to work with individual IT project owners, IT support vendors, IT officials and business users to create a list of all valuable assets. The information assets shall include hard copies of information, electronic files, removable media, mobile devices and intangibles, such as intellectual property etc. For each asset, bidder has to gather the following information, or any other information as applicable:

- Software
- Hardware
- Data
- Interfaces
- Users
- Support personnel
- Purpose
- Criticality
- Functional requirements
- IT Security policies
- IT Security architecture
- Network topology
- Information storage protection
- Information flow
- Technical security controls
- Physical security environment
- Environmental security

Bidder is required to identify mission-critical assets. Bidder needs to define a standard for determining the importance of each asset. Common criteria may include the asset's monetary value, confidentiality, legal standing and importance to SEBI but bidder is required to identify more such criteria. Once the standard

has been approved by SEBI and formally incorporated into the risk assessment security policy or appropriate document, bidder has to use it to classify each asset identified as critical, major or minor.

3.2 System Characterization

Bidder has to Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.

With respect to critical data, either in hard copy or in soft copy, bidder has to determine data classification categories. These categories shall be based on

- non-public personal information;
- data that should be restricted to a limited number of employees;
- data that should be restricted from non-employees;
- data relied upon for risk management or decision-making purposes; and
- data that is critical to the internal operations.
- data that has commercial value

The way data is categorized, same way inventoried systems are required to be classified. After classification of inventoried systems, initial risk has to be determined. Initial risk shall be **highest initial risk, medium initial risk** and **low initial risk.**

Out of these inventoried systems, bidder has to identify technology groups such as Windows Servers, Linux servers, network switches of same make and model, databases etc. Once technology groups are identified, it is required to map them with risk classification along with vulnerabilities identified with the technology group.

3.3 Threat Identification

A threat is anything that could exploit a vulnerability to breach security and cause harm to the organization. Bidder is required to identify all such potential threat events, relevance of the events, and the threat sources that could initiate the events. While identifying the malicious behavior, bidder shall consider following:

- **Channels; that a computer resources in SEBI can be accessed internally or externally.**
- **Interference**; when somebody causes damage by deleting data, engineering a distributed denial of service (DDOS) against website, physically stealing a computer or server, and so on.

- **Interception;** classic hacking.
- **Impersonation;** misuse of someone else's credentials, which are often acquired through social engineering attacks or brute-force attacks, or purchased on the dark web.

Bidder has to work with individual IT project owners, IT support vendors, IT officials and business users to identify threats.

3.4 Vulnerability Identification

Bidder is required to identify vulnerabilities both internal and external to SEBI and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts. For each identified technology group, bidder is required to assign vulnerability and threats associated with it. Vulnerabilities can be identified through vulnerability analysis, audit reports, VAPT reports, the NIST vulnerability database, vendor data, CERT-In security alert, and system software security analysis. Testing the IT system is also an important tool in identifying vulnerabilities. Testing shall include the following:

- Information Security Test and Evaluation (ST&E) procedures
- Penetration testing techniques
- Automated vulnerability Scanning tools

The sources consulted shall include:

- SANS Top 20 (www.sans.org/top20/)
- OWASP Top 10 (www.owasp.org/documentation/topten.html)
- NIST I-CAT vulnerability database (icat.nist.gov)
- Microsoft Security Advisories (www.microsoft.com/security)
- CA Alert service (www3.ca.com/securityadvisor)

3.5 Control Analysis

This phase includes assessment of controls already been implemented or planned, probability that they can be broken, assessment of potential loss despite the existence of such controls. Bidder is required to analyze the controls that are either in place or in the planning stage to minimize or eliminate the probability that a threat will exploit vulnerability in the system. Controls may be classified as below:

- **Non-technical controls also called management controls**; includes security policies, administrative actions, and physical and environmental mechanisms.

- **Technical controls**; computer hardware or software, encryption, intrusion detection mechanisms, and identification and authentication subsystems.

Both technical and non-technical controls can further be classified as preventive or detective controls. As the name implies, preventive controls attempt to anticipate and stop attacks. Examples of preventive technical controls are encryption and authentication devices. Detective controls are used to discover attacks or events through such means as audit trails and intrusion detection systems.

Bidder is supposed to identify desired amount and mix of controls to have an acceptable approach to address threats in different tiers (higher risk systems, medium risk systems and low risk systems). Bidder has to identify acceptable controls approach.

The output of this step is current or planned controls used for the IT system to measure the likelihood of vulnerability being exercised and reduce the impact of loss. The output is required to be shared with SEBI.

3.6 Identify Threat-source / Vulnerability Pairs

Bidder is required to identify all existing threat- source and associated vulnerability pairs. Bidder is supposed to develop threat scenarios which is analytically useful, since some vulnerabilities may not be exposed to exploitation unless and until other vulnerabilities have been exploited. Bidder is required to identify how a set of vulnerabilities, taken together, could be exploited by one or more threat events. Such analysis is therefore more useful than the analysis of individual vulnerabilities.

3.7 Determine the Likelihood of an incident

Bidder is supposed to determine the likelihood that threat events of concern result in adverse impacts, considering:

a. the characteristics of the threat sources that could initiate the events;
b. the vulnerabilities/predisposing conditions identified; and
c. the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Bidder is required to use following categories to assess the likelihood of an attack or other adverse event:

Likelihood level (Weight Factor)	Likelihood definition
High (1.0)	The threat source is highly motivated and sufficiently capable

	and controls to prevent the vulnerability from being exercised are ineffective
Medium (0.5)	The threat source is motivated and capable but controls are in place that may impede the successful exercise of the vulnerability.
Low (0.1)	The threat source lacks motivation or capability or controls are in place to prevent or at least significantly impede the vulnerability from being exercised.

3.8 Impact Analysis

Bidder has to determine the adverse impacts from threat events of concern considering:

a. the characteristics of the threat sources that could initiate the events;
b. the vulnerabilities/predisposing conditions identified; and
c. the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Impact analysis should include the following factors:

- The mission of the system, including the processes implemented by the system
- The criticality of the system, determined by its value and the value of the data to the organization
- The sensitivity of the system and its data

The information required to conduct an impact analysis can be obtained from existing organizational documentation or from the newly framed documents as part of the overall scope of this EOI, including a business impact analysis (BIA). This document uses either quantitative or qualitative means to determine the impact that would be caused by compromise or harm to SEBI's information assets.

An attack or adverse event can result in compromise or loss of information system confidentiality, integrity and availability. As with the likelihood determination, the impact on the system can be qualitatively assessed as **high, medium** or **low**.

The following additional items should be included in the impact analysis:

- The estimated frequency of the threat's exploitation of a vulnerability on an annual basis
- The approximate cost of each of these occurrences
- A weight factor based on the relative impact of a specific threat exploiting a specific vulnerability

3.9 Risk Determination

Bidder is required to determine the risk to the organization from threat events of concern considering:

a. the impact that would result from the events; and
b. the likelihood of the events occurring.

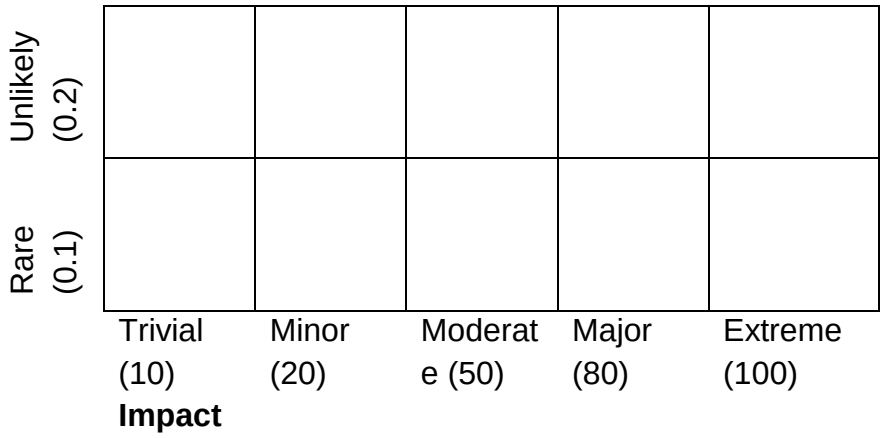
Risk = Threat Likelihood × Magnitude of Impact

For each threat/vulnerability pair, bidder has to determine the level of risk to the IT system, based on the following:

a. The likelihood that the threat will exploit the vulnerability
b. The impact of the threat successfully exploiting the vulnerability
c. The adequacy of the existing or planned information system security controls for eliminating or reducing the risk

Bidder is required to prepare risk-level matrix which shall include following:

Threat Likelihood					
Very Likely (1.0)					
Likely (0.8)					
Moderate (0.5)					



A high likelihood that the threat will occur shall be given a value of 1.0; a medium likelihood shall be assigned a value of 0.5; and a low likelihood of occurrence shall be given a rating of 0.1. Similarly, a high impact level shall be assigned a value of 100, a medium impact level 50, and a low impact level 10. Risk is calculated by multiplying the threat likelihood value by the impact value, and the risks are categorized as high, medium or low based on the result.

Bidder is required to calculate **Risk Score** for each likelihood of threat and impact of the threat.

3.10 Control Recommendations

Bidder is required to recommend controls that could mitigate or eliminate the identified risks appropriate to SEBI's operations. The control recommendations are the results of the risk assessment process.

Using the risk level as a basis, bidder has to determine the actions that senior management and other responsible individuals must take to mitigate the risk. Bidder may recommend some general guidelines for each level of risk, which may be as follows:

- **High**— A plan for corrective measures should be developed as soon as possible.
- **Medium** — A plan for corrective measures should be developed within a reasonable period of time.
- **Low** — The team must decide whether to accept the risk or implement corrective actions.

While recommending controls to mitigate each risk, bidder is required to consider:

- Organizational policies
- Cost-benefit analysis

- Operational impact
- Feasibility
- Applicable regulations
- The overall effectiveness of the recommended controls
- Safety and reliability

3.11 Results Documentation

The final step in the risk assessment process is to develop a risk assessment report to support management in making appropriate decisions on budget, policies, procedures and so on. Bidder is expected to prepare risk assessment report and present it to SEBI.

For each threat, the report should describe the corresponding vulnerabilities, the assets at risk, the impact to the IT infrastructure, the likelihood of occurrence and the control recommendations.

The results may be summarized as per following table:

SN	Observation	Threat-Source/ Vulnerability	Existing Controls	Likelihood	Impact	Risk Rating	Recommended Controls

The risk assessment report shall be comprised of all sub-sections from 3.1 to 3.11.

Bidder is expected to prepare **Risk Assessment Policy** that defines what SEBI must do periodically (preferably annually), how risk is to be addressed and mitigated, and how SEBI must carry out subsequent enterprise risk assessments for its IT infrastructure components and other assets. Bidder is required to suggest effective control measures to bring down high risk area to within tolerable residual risk value.

4. After completion of risk assessment, bidder is expected to review all the existing policies and SOPs.

Policy Documentation

5. Bidder is supposed to prepare

    5.1 General IT policies applicable to all computer resources, users across SEBI and projects (scope of work is explained in detail below), and
    5.2 for each SEBI project, an umbrella Project Policy Document (Integrated Project Manual) which identifies all applicable SEBI-wide IT policies, with specific instantiations, customizations, enhancement and exemptions needed for the underlying processes, principles and controls.

6. Bidder is required to gather details for documentation of Project Policy Document (Integrated Project Manual) and its processes through meetings and interactions with individual IT project owners, IT support vendors, IT officials and business users of SEBI.

7. Bidder is supposed to review all IT systems implemented in SEBI and prepare a comprehensive list of all the policies required by and/or recommended for SEBI. Selected bidder is expected to prepare and/or review both general IT policies and project specific IT policies which explain various underlying processes, principles and controls. These processes, principles and controls together shall constitute a secure, safe and objective operational area for the IT operations and shall drive and converge into standard operational procedures for the area. Main focus of these policies are as follows.

    7.1 Coverage: Each policy shall cover SEBI's all computer resources and users including employees (permanent or contract), vendors, outsourced staff, other third parties and individuals wherever applicable.
    7.2 Project wise or operational unit wise plan: Each policy shall have organizational level operational unit or project wise plan which will be reviewed periodically. This shall ensure maximum coverage of operating procedures followed or to be followed in each project.
    7.3 Responsibility matrix: One of the important aspects of effective operation of IT is identification of clear and non-ambiguous responsibility matrix of IT operations. Project wise plan of each policy should contain responsibility matrix for performing each IT operation in that project.
    7.4 Plan wise procedures: Each IT operation and procedures in each plan need to be identified and documented. Bidder should identify feasibility of automating each procedure and suggest usage of software scripts or tool for automation wherever practical.
    7.5 Delegation of power: Accountability is another important aspect of efficient IT operation. To execute each identified operation by the responsible professionals, appropriate authorization is envisaged through delegation of

power. Project wise plan of each policy should contain delegation of power for authorizing and approving each IT operation in that project.

7.6 Standardized forms: Many of the operational areas share common procedures for request, approval, communication etc. Each policy should incorporate standardized forms, procedures, etc. wherever practicable.

7.7 Periodic review: Each policy should identify and provide areas of operations, events, statistics, etc. for periodic review for enhancing the efficiency of operations.

8. The approach for policy development will be bottom-up policy development method. This will ensure to address the concerns of operational employees because it starts with their input and concerns, and builds on known risk.

8.1 Identification of project activities: Each policy document should include project specific activities and exceptions, handled by the project owners. Bidder is required to work with individual IT project owners, IT support vendors, IT officials and selective business users to identify and create list of clear activities, tasks, milestones or deliverables for each project.

8.2 Mapping of project wise activities: Bidder is supposed to map each activity identified within a project to appropriate policy. If any of the identified activity does not correspond to any general IT policy, then a project specific policy or procedure needs to be created and mapped appropriately.

8.3 Mapping of responsibility: Bidder is required to map each identified activity, task, milestone or deliverable within a project to a role to design responsibility matrix and accountability. This step should result into a matrix like below:

Project Name 1

Table 1: RACI Matrix

	Role 1	Role 2	Role 3	Role 4	Role 5	Role 6
Task 1	R		A	C	I	
Task 2		R	A		I	
Task 3			A		R	I
Task 4			A			R
Task 5			A		I	R
Task 6			A		I	R

9. Bidder may use a Responsibility Assignment (RACI) matrix or any other matrix as per best suitability or best industry practices. Bidder shall identify and assign Responsible, Accountable, Consulted and Informed roles for each task. Every task or deliverable should have a Responsible and Accountable at least. Only one name or role should be assigned to Accountable.

The organization structure in SEBI is as stated below:

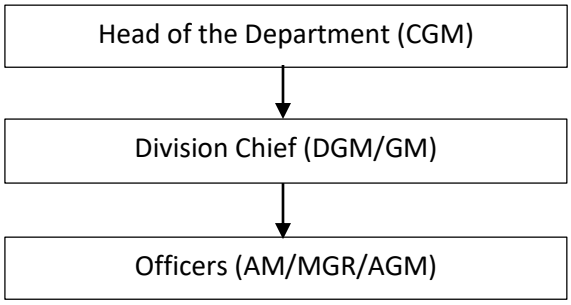


Table 2: Project wise Activity Mapping Chart A

Project Team	Activity	Type	Mapping
Officer	Task 1 Task 3 Task 4 Task 5	Responsible	Policy A Policy C Policy D
Division Chief	Task 1 Task 2	Accountable	Policy A Policy B
Head of the Department	Task 5	Consulted	Policy E Policy F

Selected bidder is expected to prepare and/or review below mentioned indicative (not exhaustive) list of policies.

A	**Information Technology Policies**		
1	IT Assets Administration and Management Policy		
2	Access Control / Management & Review Policy		
3	Capacity Planning	IT Human Resource	Management
			Training
			Skill set development

		IT Infrastructure (Servers, Desktops, Data Centers, Network Devices, Storage, Bandwidth and other equipment)
4	Application Development	Development Lifecycle Policy
		Secure SDLC
		Quality Assurance
		User Acceptance Test
		Non-functional tests (stress test, application security, destructive test etc.)
		Version Management
		System Audit
		In-house development
		Third party development
5	Data Sharing Policy	
6	Bring Your Own Device (BYOD) policy	
7	Network Access Policy	
8	Desktop Data Backup Policy	
9	Software Upgrade Policy	
10	Internet and Email Usage Policy	
11	Account and User Rights Management Policy	
12	Change Management Policy	
13	Patch Management Policy	
14	Password Management Policy	
15	Internet Security Policy	
16	Data Backup, Recovery & Restoration Policy	
17	Disaster Recovery and BCP Policy	
18	Logging and Monitoring Policy	
19	Business Requirement Collection and Documenting Policy	
20	Computer Resource Installation and Application Implementation Sign Off Policy	
21	Information Technology Incident Management Policy	
22	Configuration Management Policy	
23	Mobile Computing Policy	
24	Virtualization Management Policy	
25	Data Migration Policy	
26	Log and Record Retention Policy	
27	System Acquisition, Configuration and Maintenance Policy	
28	Network Operation Center Policy	
29	Private Cloud Management Policy	

30	IT Compliance & Review Policy	
31	Third-Party System Installation Policy	
32	Downtime Management Policy	
B	**IT Governance and Management Policies**	
1	IT Service Management	IT Governance
		Enterprise Architecture
		Project Management
		IT Budget
2	Procurement	Purchase Policy
		Equipment Allocation, De-allocation & Relocation
		Equipment Usage, Maintenance and Security
		IT Obsolescence Management
3	IT Risk Management and Supervision	
4	IT Service Request / Service Desk / Help Desk Management /Support Policy	
5	IT Service Level Agreement Policy	
6	IT Vendor Management Policy	
C	**Cyber Security Policies**	
1	Cyber Security Policy	
2	Internet Connection, Firewall, IDS & IPS Security Policy	
3	IS Compliance Policy	
4	Antivirus Management Policy	
5	Email Communication Policy	
6	Privacy Policy	
7	Third-Party Security Policy	
8	Social Media Usage Policy	
9	Communications Security Policy	
10	Internet and Intranet Policy	
11	Privileged Account Management Policy	
12	Outsourcing Policy	
13	Information Security aspects of Business Continuity Management	
14	Information Security Training and Awareness Policy	
15	Cyber Security Incident Management Policy	
16	Application Security Policy	
17	Endpoint Security Policy	
18	Operating System Security Policy	
19	Database Security and Access Policy	
20	Web Server Security Policy	

21	Mobile Application Security Policy
22	Cloud Computing and Security Policy
23	Security Operation Center Policy
24	Acceptable Use of Assets and Controls Policy
25	Remote Access Policy
26	Website Content Update Policy
27	Data Governance and Classification Policy
28	Data Leakage Prevention Policy
29	Data Retention Policy
30	Risk Assessment and Risk treatment Policy
31	Statement of applicability (SoA)
32	Cryptography Policy
33	Physical & Environmental Security Policy
34	Segregation of Duties Policy
35	Wireless Policy
36	VPN Security Policy
37	Telecom Security & Related Equipment Controls Policy
38	Digital Signatures Policy
39	Media Controls Policy
40	Intellectual Property Rights Security Policy
41	Legal Requirements & Compliance Controls Policy
42	Data Centre Security Policy
43	Personnel Security Policy
44	Server Security Policy
45	Data Breach Response Policy
46	End User Encryption Key Protection Policy
47	Ethics Policy
48	Pandemic Response Planning Policy
49	Security Response Plan Policy
50	Email Retention Policy
51	Extranet Policy
52	Server Audit Policy
53	Server Malware Protection Policy
54	Social Engineering Awareness Policy
55	Clean Desk Policy
56	Router and Switch Security Policy
57	DMZ Security Policy
58	Internet DMZ Equipment Policy
59	Mobile Device Management & Encryption Policy

60	Personal Communication Devices and Voicemail Policy

Sample template for the policy: *A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent, and is implemented as a procedure or protocol.*

S/No	Policy Template Headings	Description
1	Policy Objective	A policy objective is a desired outcome that is required to achieve with this policy.
2	Scope and Applicability	An applicability and scope statement, describing who the policy affects and which actions are impacted by the policy. The applicability and scope may expressly exclude certain people, organizations, or actions from the policy requirements. Applicability and scope is used to focus the policy on only the desired targets, and avoid unintended consequences where possible.
3	Ownership	Ownership defines primary responsibility and accountability for this policy and its associated tasks.
4	Policy description	Policy description is the set of guidelines or rules that determine a course of action.
5	Project wise plan	Project wise activity mapping chart and exception handling for each project applicable to this policy.
	a. Responsibility Assignment matrix	RACI matrix (Table 1 as mentioned above)
	b. Activity mapping chart	Activity mapping chart (Table 2 as mentioned above)
	c. Process/Procedures	A standard operating procedure (SOP) is a set of step-by-step instructions compiled to carry out complex routine operations.
6	Policy references	References to other policies and procedures
7	Policy Compliance	Compliance to the rules as documented in the policy description
8	Framework for policy implementation	Framework for effective implementation of policies. Such matrix should contain quantitative and qualitative representation and turnaround time for policy implementation so that SEBI will use such matrix in future to evaluate the SOP prepared. The policy should contain

S/No	Policy Template Headings	Description
		framework for implementation. This framework should be aligned with the project plan for the successful implementation of the policy.
9	Training and Awareness	Define schedules for Training and Awareness on policy, if applicable, and plans including training to new employee and outsourced resources.
10	Waivers and breaches	Exception handling
11	Maintenance, Review & Continual Improvement	On what all occasions policy document will be updated, who will review the policy and with what frequency. It will identify who is authorized to initiate change request to update the policy and who shall review this change request.
12	Exhibits / Appendices / Forms	Supplemental information to the policy such as lengthy or complex reference information that would disrupt the flow of other sections. Any form required by the policy for collecting certain data. Any supplementary material referred. Ex. Standard Computer Resource Access Form, User Creation Form etc.

	Guidelines
1	Device hardening guidelines
2	Patch management guidelines
3	Anti-virus / malware guidelines
4	User Access Management guidelines
5	Privilege access management guidelines
6	End point management guidelines
7	Connectivity guidelines for Trading partners and external agencies
8	Controls on mobile devices and wireless technology
9	Password Construction Guidelines
	Standards
1	Information Logging Standard
2	Wireless Communication Standard
3	Malicious Code Protection Standard

Standard Operating Procedure Documentation

10. Statements in each policy should be able to converge into standard operating procedures. Combined with responsibility matrix and delegation of power, these standard operating procedures should provide actual work which will be carried out daily in a project. Further these standard operating procedures should be prepared in such a way that they can be reviewed and enhanced without changing the policies. Also, by dividing these standard operating procedures of each policy among projects along with responsibility matrix and delegation of power, project wise daily operation procedures should be prepared. SOPs should cover all IT operations across SEBI.

11. **Standardizations**

    All the procedures and processes need to be standardized wherever practicable. Addition, deletion and enhancements of standardized forms and procedures should be achieved as and when required without amending the policies or standard operating procedures.

12. Selected bidder is expected to prepare and/or review below mentioned indicative (not exhaustive) list of Standard Operating Procedures (SOPs). These SOPs can be for general IT policies or for project specific IT policies. The bidder should examine each procedure and should determine in which policy they come into. If it not falls into any of the policy bidder should create appropriate custom policy to cover the operations.

A	**Standard Operating Procedure for General IT Policies**
1	Asset Management Procedure (Including Identification & Classification of Information Assets)
2	Access Control, Management & Review Procedure
3	Capacity Planning and Management Procedure
4	Application Development Procedure
5	Data sharing SOP
6	Bring Your Own Device (BYOD) SOP
7	Network Access Procedure
8	Desktop Data Backup Procedure
9	Software Upgrade and Patch Management SOP
10	Internet and Email Usage SOP
11	Account and User Rights Management Procedure
12	Change Management Procedure
13	Patch Management Procedure
14	Password Management Procedure

15	Internet Security process
16	Data Backup, Recovery & Restoration Procedure
17	Disaster Recovery and BCP Procedure
18	Logging and Monitoring Procedure
19	Business Requirement Procedure
20	Computer Resource Installation and Application Implementation Sign Off Procedure
21	Information Technology Incident Management Procedure
22	Configuration Management Procedure
23	Mobile Computing SOP
24	Virtualization Management Procedure
25	Data Migration SOP
26	Log and Record Retention SOP
27	System Acquisition, Development and Maintenance SOP
28	Network Operation Center SOP
29	Private Cloud Management SOP
30	IT Compliance & Review Process
31	IT Risk Assessment and Management Procedure
32	IT Service Management Procedure
33	SOP for IT Procurement
34	IT Help Desk Management Procedure
35	IT Service Level Agreement Process
36	IT Vendor Management Process
37	Cyber Security SOP
38	Internet Connection and Firewall SOP
39	IS Compliance Procedure
40	Antivirus Management Procedure
41	Email Communication Procedure
42	Privacy SOP
43	Third-Party Security SOP
44	Social Media Usage SOP
45	Communications Security Procedure
46	Internet and Intranet Procedure
47	Privileged Account Management Procedure
48	Outsourcing Procedure
49	Information Security aspects of Business Continuity Management process
50	Information Security Training and Awareness SOP
51	Cyber Security Incident Management Procedure
52	Application Security Procedure

53	Endpoint Security SOP
54	Operating System Security SOP
55	Database Security and Access SOP
56	Web Server Security SOP
57	Mobile Application Security SOP
58	Cloud Computing and Security SOP
59	Security Operation Center SOP
60	IT Assets/Media Disposal Procedure
61	Third-Party System Installation Process
62	Downtime Management Process
63	Remote Access Process
64	Website Content Update Process
65	Data Governance and Classification Process
66	Data Leakage Prevention Process
67	Data Retention Process
68	Risk Assessment and Risk treatment Process
69	Statement of applicability (SoA) Process
70	Cryptography Process
71	Physical & Environmental Security Process
72	Segregation of Duties Process
73	Wireless Process
74	VPN Security Process
75	Telecom Security & Related Equipment Controls Process
76	Digital Signatures Process
77	Media Controls Process
78	Intellectual Property Rights Security Process
79	Legal Requirements & Compliance Controls Process
80	Data Centre Security Process
81	Personnel Security Process
82	Server Security Process
83	Data Breach Response Process
84	End User Encryption Key Protection Plan Process
85	Ethics Procedure
86	Pandemic Response Planning Process
87	Security Response Plan Process
88	Email Retention Process
89	Extranet Process
90	Server Audit Process
91	Server Malware Protection Process

92	Social Engineering Awareness Process
93	Clean Desk Process
94	Router and Switch Security Process
95	DMZ Security Process
96	Internet DMZ Equipment Process
97	Mobile Device Management & Encryption Process
98	Personal Communication Devices and Voicemail Process

B	**Application Specific Standard Operating Procedures**
B.1	**ERP**
1.	Payroll process for HO, RO and LO
2.	Taxation and FORMs 16 process
3.	37 type of Claims Process for HO, RO and Los
4.	Leave & Attendance Management Process
5.	Annual Performance Appraisal Process
6.	Personnel Administrations Process
7.	Organization Management Process
8.	International and Domestic Travels including Forex process
9.	Provident Fund & Statutory reports process
10.	PF-Treasury and Risk Management
11.	Loans Process
12.	Annual Returns and Investment Declaration process
13.	Leave Fare Concessions process
14	Account Payables Process
15	Account Receivables Process
16.	General Ledger Process
17.	Cash Management Process
18.	TDS process
19.	Budget process
20.	Fixed Assets process
21.	Treasury and Risk Management process
22.	Material Management Process
23.	SAP Basis process
24.	Financial Statements Process
25.	Travel related process (domestic and international)
26.	APAR process
27.	Investment declaration process
28.	HR (Time, leave, attendance, PI info, Master data, etc) Related Process

B.2	**SHARE Portal – Employee specific**
1.	IBM FORMS process
2.	IBM Connections Process
3.	Contents Uploading Process
4.	Contents Creation
5.	Holiday home booking process
6.	Vendor Bill Payment process
7.	Conference room booking process
B.3	**Document Management System**
1.	Inward of document
2.	Outward of Document
3.	Initiate Office Note
4.	Circular Number Generation
5.	File Number Generation
6.	Scanning of Document and attaching with the Office Note
7.	Backlog Scanning and Verification
8.	File Tracking - Outward / Inward / Office Note
9.	Transfer of documents from officer / other officer
10.	Transfer of document from one department / division to other department / division
B.4	**SEBI Website**
1.	Creation/updating of sections and sub-sections and their contents.
2.	Creation of users in the CMS
3.	Updating of users in the CMS
4.	Visit to SEBI
5.	Integration with SHARE portal through web services
6.	Integration with Case Management System through web service
7.	Creation/updating of content/data/links/section/subsection etc.
8.	Vulnerability Assessment and Penetration Testing (VAPT) for SEBI website
9.	Disaster Recovery Drill
10.	Performance Testing
11.	Security Incidents and Risk mitigation
B.5	**SHARE Portal E-Registration**
1.	Self-registration and login procedure
2.	e-registration procedure

3.	Process for Payment of various fees by intermediaries
4.	Post registration activities
5.	Submission of periodic reports
6.	Submission of risk-based report
7.	Process for payment reconciliation with SEBI Accounts
8.	Form-A generation procedure
9.	Calculation of fees and interest liability for Stock Brokers
10.	Process for resolving historical data migration issues
11.	Process for portal password reset where email ID/mobile no are not valid
B.6	**Email System**
1.	Process for account creation, space allocation
2.	Process for email blocking, email sending to group
3.	Moderator for release of email
4.	Email retention process
5.	Email process after retirement/resignation
6.	Email permission to other user within division for accessing in case of leave/resigned/suspension
7.	Creation of Group email
8.	Deactivation of public email
9.	Email Archival process (pst file)
10.	Delegating Access to generic email in outlook
11.	Process for Restoring Email from GFI Archiver
12.	Process for Registering / Change in mobile no for OTP
B.7	**IP telephony and networking**
1.	SLA compliance procedure
2.	IP phone allocation process
3.	STD/ISD provision
4.	Call record retention process
5.	Network log maintenance/retention process
6.	Configuration / acceptance process
7.	WIFI Access policy
B.8	**IT Assets**
1.	Allocation of IT related assets during on-boarding of employee
2.	Allotment and procurement of IT asset for Senior Management
3.	Data backup and transfer
4.	Process for data retention

B.9	**Case Management System**
1.	Case Registration
2.	Adjudication
3.	Enquiry
4.	11B
5.	Prosecution
6.	Recovery
7.	SAT
8.	LAD
9.	LBP
10.	Compounding
11.	Settlement
12.	Process for Penalty Payment
B.10	**SCORES System**
1.	SCORES website
2.	CPGRAMS module
3.	Inwards module
4.	Admin module
5.	Staff module
6.	Mobile App
7.	Intermediary module
B.11	**IMSS and DWBIS**
1.	Data acquisition procedure
2.	Data reconciliation procedure
3.	Data Transformation procedure
4.	Data processing procedure
5.	Scripting
6.	Data Transfer procedure
7.	Data Validation procedure
8.	Data Loading procedure
9.	Data Movement procedure
10.	Alert generation procedure
11.	Alert management procedure
12.	Data sync procedure
13.	Data Backup procedure
14.	Logs management

15.	Monitoring and management of hardware, software etc.
16.	Daily check list verification
17.	End of day summary verification procedure
18.	Digital certificate management
19.	User management
20.	Generation of SEBI Bulletin
21.	Change Request Management
22.	Helpdesk management
23.	Business User reports and issue resolution
B.12	**Security Operations Center**
1.	Exception mail handling process
2.	Firewall Security process
3.	Process for mobile antivirus
4.	Malware scanning process
5.	Process for SOC application management
6.	Process for addition of rules in SOC technologies
7.	Process for user system quarantine
8.	Exception management for SOC technologies
9.	Fine tuning process
10.	User complaint resolution process
11.	Defect management process
12.	File upload whitelisting process
13.	Critical security event management process
14.	True incident management process
15.	Process to build knowledge store
16.	Privileged account lifecycle process
17.	User group management process
18.	Permission assignment process
19.	Process for auditing of logs
20.	Structured monitoring process
21.	Review process
22.	Forensic analysis process
23.	Suspicious/malicious email reporting and management
24.	SLA compliance procedure
25.	Behavioral monitoring process

13. The Responsibility Assignment matrix should be included in the SOP document for each policy. The output expected is as follows:

13.1 Standard Operating Procedure for each policy
13.2 Standard Operating Procedure for project

14. The anticipated structure of the policy and SOP is as follows:
    14.1 SOP for each policy
        14.1.1 Project wise process, procedure, calendar and schedules
        14.1.2 Activity mapping and Responsibility Assignment matrix
        14.1.3 Delegation of power

    14.2 Project wise SOP
        14.2.1 Daily work by Officer, Division Chief (DC), Head of the Department (HoD)
        14.2.2 Weekly Plan
        14.2.3 Monthly Plan
        14.2.4 Yearly Plan

The project wise SOP shall have following activity mapping chart:

Table 3: Project wise Activity Chart B

Task/ Activity	Responsible	Accountable	Consulted	Informed	Frequency (Daily/ Weekly/ Monthly/ Yearly)
Task 1	Officer/DC	DC/HoD	Officer/DC/ HoD	DC/HoD	D/W/M/Y
Task 2	Officer/DC	DC/HoD	Officer/DC/ HoD	DC/HoD	D/W/M/Y
Task 3	Officer/DC	DC/HoD	Officer/DC/ HoD	DC/HoD	D/W/M/Y

Table 4: List of tasks

Task/ Activity	Sub-tasks	Automatic	Manual	Name of Software Scripts or Tools
Task 1	Sub-task1	Y	N	
	Sub-task 2	N	Y	
	Sub-task 3	Y	N	
	Sub-task 4	Y	N	

Task 2	Sub-task1	N	Y	
	Sub-task 2	N	Y	
	Sub-task 3	N	Y	
	Sub-task 4	Y	N	

15. Each policy and process/procedure document shall have Table 1, 2, 3 and 4 to depict clear identification of task and assignment as per responsibility matrix and delegation of power. Bidder can propose best way of representation of these tables as per the industry standards.

16. SOPs shall have calendar and scheduler defined to identify when a particular task is required to be initiated and completed.

17. Bidder is expected to provide comprehensive list of policies and list of SOPs and procedures to support the policies along with the frameworks where the SOP draws their processes from and how they relate, for all the policies identified. Bidder is required to examine each procedure in detail, identify which software scripts or tools are required to run the procedure, recommend SEBI what is the extent of automation possible and provide recommended software scripts or tools for the procedures. SOP's should be designed to create uniformity of effort, and cohesion, thus resulting in the continuity of standards/policies. The aim of SOP documentation is to couple objectives with standards/policies and for “tactical” implementation of the standards/policies.

    Sample template for SOPs

A process is a sequence of activities that convert an input into a valued output (or outcome).

S/No	Process Template Headings	Description
1	Process objective	Process Objectives focus on the activities to be completed in a specific time period. Process objectives support accountability by setting specific activities to be completed by specific dates and explain what and when it will be completed.
2	Process goal	Process goal is defined as what is required to achieve.

S/No	Process Template Headings	Description
3	Scope	Scope of a process is to identify the applicability and activities covered for the process.
4	Entry criteria	Activities which can trigger this process.
5	Inputs	Inputs which can be referred to complete the process or activity.
6	Process flows	The Process Flow chart provides a visual representation of the steps in a process.
7	Activities	Activities or tasks identified in the process
	a. Responsibility Assignment matrix	RACI matrix considering delegation of power
	b. Activity mapping chart	Activity mapping chart (Table 3 as mentioned above)
	c. List of automatic or manual tasks	List of automatic or manual tasks (Table 4 as mentioned above)
8	Verifications	Evaluation or review
9	Measurements	The specific steps in a process that lead — either positively or negatively — to a particular outcome metric.
10	Scorecard for process evaluation	Scorecard for effective implementation of SOPs. SOP should contain a scorecard for evaluation and proof of evidence for every compliance point of policy.
12	Exit Criteria	Criteria or requirements which must be met to complete a specific task or process.
13	Process Output	The result (the product/service) produced by the process.
14	References	References to other policies and procedures
15	Exhibits / Appendices / Forms	Any supplementary material referred or forms used.

18. Process flows: The Process Flow chart provides a visual representation of the steps in a process. The document shall cover actual steps required to be

performed and not the escalation matrix. Process flow must depict a visual representation of the sequence of steps and decisions needed to perform for a process. All process flows must incorporate flows for normal steps as well as exceptional flows. The process flow chart shall cover each possible exception in the flow and add decision node for the alternative solution path.

19. SEBI intends to automate the processes identified for accuracy and error free execution of task. The decision on the extent of automation will be decided by SEBI and its technical advisory committee members. Bidder is responsible for identification of processes, its documentation and design specifications. Implementation of the automation required is not part of the scope of this EOI.

20. Policy and SOP documents should be prepared in accordance with ISO 27001, 22301 standards. Bidder is supposed to provide recommendations on Standards and frameworks required to be followed like COBIT, ISO, and ITIL etc. It is required by the bidder to specify which elements of the standard and /or framework may not be necessary for SEBI.

21. The policy documents need to be segmented and flexible enough to incorporate standards and frameworks as well as limitations due to legacy systems. For example: The parameters for segments can be Security system and Critical system.

22. The policy documents must be adequately detailed so that it becomes specifically actionable for SEBI. For example: Password Management

22.1 Suppose SEBI systems can be accessed from SEBI network and also through Virtual Private Network (VPN) when accessing through Internet, then for these two ways of access following categories might be applicable:

22.1.1 **Single Factor Authentication: When accessing SEBI systems from SEBI network.** Systems categorized on the basis of critical to less critical then password characteristics can be documented as below:

Cat I	validity of 6 months; 2 passwords to be kept in history
Cat II	alphanumeric; validity of 3 months; 3 passwords to be kept in history
Cat III	alphanumeric with 1 special character and one number; validity of 1 month; 5 passwords to be kept in history

*Please note these are just illustrations to explain the granular approach expected by SEBI while preparing the documents.

22.1.2 **Two Factor Authentication: When accessing SEBI systems through VPN**

Cat I	Strong Password + One Time Password (OTP) via SMS
Cat II	Strong Password + One Time Password (OTP) via Voice

*Please note these are just illustrations to explain the granular approach expected by SEBI while preparing the documents.

23. Bidder is expected to provide comprehensive list of policies and list of SOPs and procedures to support the policies along with the frameworks where the SOP draws their processes from and how they relate, for all the policies identified. SOP's should be designed to create uniformity of effort, and cohesion, thus resulting in the continuity of standards/policies. The aim of SOP documentation is to couple objectives with standards/policies and for “tactical” implementation of the standards/policies. For example:

    23.1 Policy for Access Control –

Type 1	Rule-based Access Control
Type 2	Role-based Access Control

    23.2 SOP for Access Control Procedure should explicitly define–
        23.2.1 Who is authorized to get what level of access?
        23.2.2 Who is authorized to approve such access?
        23.2.3 How revocation should be done?

    *Please note these are just illustrations to explain the granular approach expected by SEBI while preparing the documents.

24. Bidder is supposed to prepare an audit checklist for internal purposes. This is required to identify and collect evidence of compliance by means of logs or any other method. The checklist should be based on defined roles with daily / weekly / monthly / annual compliance.

25. Since all policies should be stakeholder focused, it is required that the policies need to be cross referenced with the SOPs.

26. Bidder is expected to provide deliverables in a phased manner. Thus, two weeks after commencing the contract, bidder is expected to review all IT systems and prepare comprehensive list of policies and SOPs as mentioned above, bidder will also prepare document for phase wise delivery of policies and SOPs.

27. It is required by the bidder to review all existing documents and update them as per industry standards and/or in line with organization level policy documents. Also, it might be required by the bidder to prepare many of these documents afresh. Selected bidder is expected to verify and update, if required, existing policies/SOPs/documents so that these documents will also get standardized as per industry standards.

28. All IT policies should have following sections:

28.1 Policy Management

Selected bidder is expected to provide recommendations on different kinds of tools and/or systems required to manage all these processes and monitor compliance with both policies and SOPs. Such tool should have centralized repository where policies can be developed, created and maintained. This repository should serve as the hub to keep all policies easily accessible, with an audit trail.

28.2 Application of the Policy

The documentation activity should cover all Information Technology processes for:

a) Normal/Ordinary course of events
b) Failure mode
c) Emergency mode.

28.3 Review of the Policy

The review section of each policy should mention when the review of the said policy required to be carried out:

a) Time based review: Annual review or Comprehensive review in every 3 years.
b) Major change request based review
c) Other policy has an impact – dependent policy undergoes changes

28.4 Dependency on other policies

This section should explicitly mention dependency of other policies. For example: Information Security policy has dependency on Access control policy, Asset Management policy, etc.

The reference section should mention policy and SOP referred.

29. Standards

Policies and Standard Operating Procedures (SOPs) are required to be designed as per best industry standards and practices including identifying processes that should be automated using scripts. The policy should clearly mention which standard being followed while preparing the policy.

Design Specification for Process Automation

30. SEBI intends to automate the processes identified for accuracy and error free execution of the tasks/activities. Bidder is required to identify all such processes

which can be automated fully and/or partially. The decision on the identified processes and extent of automation will be decided by SEBI and its technical advisory committee members. Bidder is responsible for identification of processes, its documentation and preparation of design specifications. Implementation of the automation required is not part of the scope of this project.

31. Bidder is required to develop design specification document for each process and its sub-processes. Process design specifications shall involve the formal statement of the required functions, features and performance of the process to be designed. The design specification document shall provide information about the process or procedure which shall cover current status of the process, expected status of the process, exception list and SLA format.

32. Bidder is supposed to gather process details for documenting design specifications through meetings and interactions with SEBI officials and IT support vendors of SEBI. The identification of processes for automation shall be done by bidder after considering current status of the identified process. The status of the processes can be fully and/or partially manual.

33. Each SOP, procedure or process shall have a design specification document to cover all the activities and steps being performed for the underlying SOP, procedure or process. The process shall have sub-processes to cover exception handling and error situations. The processes, procedures and SOPs shall include normal process flow as well as exception flows, alternate flows and known error flows.

34. The process identified for documentation shall cover all sub-processes and their SLAs associated.

35. The design document shall include exceptions, steps taken for handling the exceptions, what is required for automation and its SLA compliance.

    Design specification is required for creating scripts for the automation of each of the system for each of the process.

    The bidder team shall prepare the Business Requirement Document for all the business process identified for design document preparation.

36. The design specification shall include following formats:

*Please note these are just illustrations to explain the granular approach expected by SEBI while preparing the documents.

Example - ETL Process for One Exchange One Segment

ETL Process starts after the market close : Usual time of receiving file startes at 1900 hours
Description of the major processes are as follows :
The detail event of the processes is explained in the Error Exception tab.

Table 1:

S/ No	Process Name	Process Description	Process Input	Process Output
1	P0: Polling Program	This will start the Source Data copy from Market server to SEBI IMSS Server	Polling Script Trigger	Source data availability on IMSS Server
2	P1: File Copy from IMSS to DWBIS	This will start the Source Data copy from IMSS Server to DWBIS Server	File Copy Scripts 1. IMSS Server to Landing Server 2. Landing Server to Staging Server	Source data availability on DWBIS Server
3	P2: Validation Process	This will do the validation and sanity check for Source data	Source data in the form of .csv/.data/zipped/unzipped Data validation Scripts (.ok file, md5sum, checksum, EODDTR)	Source files ready for further processing
4	P3: ETL Trigger	ETL will start the data processing and loading into target tables	Source files on staging server with proper file format Expected file size with proper columns and data types	Source data load started in FACT/DIM tables
5	P4: ETL Completion table updates and triggers	ETL will end up in loading the source data into target tables	ETL Transformations, logic and Database requisites	Source data loaded into FACT/DIM tables (MIG environment)
6	P5: Data movement to PRODUCTION	Data movement is the process of moving (loading) the data into Production tables	Data Movement to PROD scripts Data should be available for the respective Exchange/Segment and Respective Business Day in	Data will be available in Production database for Alert Generation

S/ No	Process Name	Process Description	Process Input	Process Output
			MIG Environment Hardware sustainability	
7	P6: Data Synchronization with ORACLE	Source data in the database tables will be in synchronization with PROD environment	Data Movement to Oracle scripts Data should be available for the respective Exchange/Segment and Respective Business Day in PROD Environment Hardware sustainability	PROD and Oracle database tables will be in sync which will reduce the data discrepancies in alerts.
8	P7: Alert Generation	Alert model will provide us the Alerts w.r.t. FR, PIT, MTC, Disclosure on Daily, Monthly, Quarterly basis	Exchange source data from production database Alert model processing logic	Alerts will be made available to the users

Table 2:

S/ No	Process ID	Error/ Exception Process ID	Name of the Process	Current Status (Manual/ Automated)	Expected Status (Manual/ Automated)	Error/ Exception	SLA Format
1	**P0**		**P0: Polling Program. The Polling program is used to copy Exchange data from Exchange server to SEBI IMSS server.**	Manual/ Automated	Manual/ Automated		**P0: ST(19:00) and ET (24:00) T+0 | Status #**
	P0.1		**P0.1: Trigger Polling program: 1900 HRS - Cron job.**	Automated	Automated	E0.1: Cron job fails:	
						E0.11: Recent system update	E0.11: ST and ET | Status # E0.11

S/ No	Process ID	Error/ Exception Process ID	Name of the Process	Current Status (Manual/ Automated)	Expected Status (Manual/ Automated)	Error/ Exception	SLA Format
						E0.12: Password expiry.	E0.12: ST and ET | Status # E0.12
						E0.13: Server issue	E0.13: ST and ET | Status # E0.13
						E0.14: Poling program already running	E0.14: ST and ET | Status # E0.14
		PE0.1	PE0.1: Run Diagnostic:	Manual	Automated		
		PE0.11	PE0.11: Check / modify system update change. Sync with NTP. Wait and retry till timeout	Manual	Automated	EPE0.11: Timeout	E0.15: ST and ET | Status # EPE0.11
		PE0.12	PE0.12: Reset password.	Manual	Automated / Manual	EPE0.12: Manual interjection. Reset Password	E0.16: ST and ET | Status # EPE0.12
		PE0.13	PE0.13: Check server logs for Error. Wait and retry till timeout	Manual	Automated / Manual	EPE0.13: Check server logs for Error. Manual interjection	E0.17: ST and ET | Status # EPE0.13
		PE0.14	PE0.14: Exit.	Automated	Automated		E0.18: ST and ET | Status # EPE0.14

S/ No	Process ID	Error/ Exception Process ID	Name of the Process	Current Status (Manual/ Automated)	Expected Status (Manual/ Automated)	Error/ Exception	SLA Format
2	**P0.2**		**P0.2: Check Network Connectivity.**			**E0.2: Network Connection not available.**	**E0.2: ST and ET | Status # E0.2**
		PE0.2	PE0.2: Raise ticket with NMS. Continue to check for Network connectivity till timeout.	Manual	Automated	EPE0.2: Timeout	E0.21: ST and ET | Status # EPE0.2
3	**P0.3**		**P0.3: Check for space.**	Manual	Automated	**E0.3: Space not available.**	**E0.3: ST and ET | Status # E0.3**
		PE0.3	PE0.3: Run diagnostic to clear old/ temp files	Manual	Automated	EPE0.3: Space not available yet. Manual interjection.	E0.31: ST and ET | Status # EPE0.3
4	**P0.4**		**P0.4: Create download directory.**	Automated	Automated	**E0.4: Not able to create download directory.**	**E0.4: ST and ET | Status # E0.4**
		PE0.4	PE0.4: Run diagnostic to Grant permission.	Manual	Automated	EPE0.4: Still not able to create download directory. Manual interjection.	E0.41: ST and ET | Status # EPE0.4
5	**P0.5**		**P0.5: FTP the files : Input is the list of files to be copied.**	Automated	Automated	**E0.5: FTP failed:**	**E0.5: ST and ET | Status # E0.5**
		PE0.51	PE0.51: check for updated credentials. Wait and retry till timeout.	Manual	Manual	EPE0.51: login failed. Timeout	E0.51: ST and ET | Status # EPE0.51

S/ No	Process ID	Error/ Exception Process ID	Name of the Process	Current Status (Manual/ Automated)	Expected Status (Manual/ Automated)	Error/ Exception	SLA Format
		PE0.52	PE0.52: check for host availability. Wait and retry till timeout.	Manual	Automated	EPE0.52: host unavailable. Timeout	E0.52: ST and ET | Status # EPE0.52
		PE0.53	PE0.53: check for file availability. Wait and retry till timeout.	Automated	Automated	EPE0.53: file busy. Timeout	E0.53: ST and ET | Status # EPE0.53
		PE0.54	PE0.54: check for connection. Wait and retry till timeout.	Manual	Automated	EPE0.54: connection reset. Timeout	E0.54: ST and ET | Status # EPE0.54
		PE0.55	PE0.55: check for user availability. Wait and retry till timeout.	Manual	Automated	EPE0.55: too many users. Timeout	E0.55: ST and ET | Status # EPE0.55
6	**P0.6**		**P0.6: Repeat P0.5 till all files are copied or till max Polling timeout.**	Automated	Automated	E0.6 : Source files still not copied / Polling timeout	PE0.6: ST and ET | Status #
		PE0.6	PE0.6: Restart Polling program	Automated	Automated		

Status # = S: Success ; F: Failure; Error Code
ST: Start Time of the process
ET: End Time of the process
P: Processes
E: Error/Exceptions
PE: Processes for Error/Exceptions
EPE: Error for Processes for Error/Exceptions

SLA format :
P0: ST(19:00) and ET (24:00) T+0 | Status # Success / Failure / EX.XX

37. Detailed scope of work will be included in the Request for Proposal (RFP) document.

SECTION V – BIDDER'S ELIGIBILITY CRITERIA

This process is open to all Bidders who fulfill the eligibility criteria as set out below and is in agreement with SEBI as per terms & conditions of this EOI document. The Bidders should furnish documentary evidence supporting the information provided by them as part of the bidding process. EOIs not satisfying the eligibility criteria will be rejected.

SN	Criteria	Details	Supporting Documents to be submitted
1	Incorporation	• The bidder should be registered as a company in India as per Company Act 1956/2013 or a partnership firm registered under LLP act, 2008 • Should have operation for a period of at least 3 years as on date of EOI.	Letter of undertaking to this effect on company's letter head signed by company's authorized signatory.
2	Location	The bidder should have registered office in India. Also bidder should have office in Mumbai Metropolitan Region from where this project will be executed.	Self-declaration with address and contact details on company's letter head signed by company's authorized signatory. For both registered office address and Mumbai Metropolitan Region office address.
3	Past relevant experience	The bidder should fulfill one of the following criteria in respect of past experience of having successfully completed similar projects over the last five years i.e. current financial year and the last five financial years: Three similar completed projects costing not less than the amount equal to INR 78,20,000/-	The submitted projects can be of following types. Scope of Work (SOW) sections (Policy preparation, Risk Assessment, SOP documentation, Process Design Specification) One set of single PO with all four SOW sections included **OR** One set of any three SOW section in one PO and

SN	Criteria	Details	Supporting Documents to be submitted
		(Seventy-Eight Lakhs Twenty Thousand only) OR Two similar completed projects costing not less than the amount equal to INR 97,75,000/- (Ninety-Seven Lakhs Seventy-Five Thousand only) OR One similar completed project costing not less than the amount equal to INR 1,56,40,000/- (One Crore Fifty-Six Lakhs Forty Thousand only).	remaining one SOW section in another PO **OR** One set of any two SOW section in one PO and remaining two SOW section in another PO **OR** One set of all four SOW section in four different PO. Each set will be considered as one completed project.
4	Fit and Proper	The bidder should not be a blacklisted firm/company in any Govt. department/Banks/ PSU/other institution in India due to unsatisfactory performance, breach of general or specific instructions, corrupt or fraudulent or any other unethical business practices.	Letter of undertaking to this effect on company's letter head signed by company's authorized signatory.
5	No conflict of interest	In order to avoid conflict of interest, bidder must not be the existing application implementer(s) and / or solution provider(s) of SEBI.	Letter of undertaking to this effect on company's letter head signed by company's authorized signatory.

SECTION VI – EOI SUBMISSION PROCESS

1. **Raising of queries/clarifications on Request for EOI document:** The Bidders requiring any clarification on this document should submit their written queries to email id: *sebiSOP@sebi.gov.in*. Any suggestions / feedback may also be sent to the above email id.

2. **Modification in Request for EOI document:** At any time prior to the deadline for submission of EOIs, SEBI may modify any part of this document. Such change(s) if any may be in the form of an addendum/corrigendum and will be uploaded in SEBI's website - https://www.sebi.gov.in. All such change(s) will automatically become part of this Request for EOI and will be binding on all Bidders. Interested Bidders are advised to regularly refer the SEBI's URL referred above for any updates.

3. Request for extension of date for submission of EOIs will not be entertained. However, to give prospective Bidders reasonable time to take the amendment into account in preparing their EOIs, SEBI may, at its discretion, extend the last date for the receipt of EOIs. No EOI may be modified subsequent to the last date for receipt of EOIs. No EOI may be withdrawn in the interval between the last date for receipt of EOIs and the expiry of the EOI validity period specified by the Bidder in the EOI.

4. Bidders are advised to study the EOI Document carefully. Submission of the EOI will be deemed to have been done after careful study and examination of all instructions, eligibility norms, terms and requirement specifications in the EOI document with full understanding of its implications. EOIs not complying with all the given clauses in this EOI document are liable to be rejected. Failure to furnish all information required in the EOI Document or submission of an EOI not substantially responsive to the EOI document in all respects will be at the bidder's risk and may result in the rejection of the EOI.

5. EOI as per format provided in Annexure II and details as per format provided in Annexure I, Annexure III, Annexure IV and Annexure VI should be submitted along with proof of documents. Further, Bidders are required to provide an estimated cost (not commercial quotes) for the project based on the scope of work mentioned above and details provided in Annexure VII in the format prescribed in Annexure V.

6. If the space in the Pro forma is insufficient for furnishing full details, the information shall be supplemented on separate sheets of paper stating therein the part of the statement and serial number. Separate sheets shall be used for each part. Any inter-

lineation, erasures, or overwriting shall be valid only if the person(s) signing the EOI initial(s) them.

7. **Submission of EOIs:** Detailed EOI has to be submitted in a sealed envelope superscripted "**EOI - Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification"** on or before January 08, 2021 at 03:00 PM. The envelope should be addressed to **Shri Manojan Karayi (Chief Information Security Officer)** and submitted at **SEBI Bhavan II, Plot No.: C7, G-Block, Bandra Kurla Complex, Bandra (East), Mumbai - 400051** before the due date and time specified. **No extension on the specified submission schedule will be entertained**.

8. SEBI may ask Bidders for clarifications or additional documents/ credentials at its discretion.

9. **Opening of EOI** – SEBI will convene the EOI opening session on duly notified date i.e. January 08, 2021 at 04:00 PM through web meeting where two representatives from the Bidders, who have successfully submitted the EOI, can participate. For web meeting invites, bidder is required to send email at *sebiSOP@sebi.gov.in* with name, email id and contact details of the representatives. The EOIs will then be passed on to a duly constituted Tender Evaluation Committee (TEC).

10. EOI so submitted should remain valid for a minimum period of 90 days from the scheduled date of opening.

SECTION VII – EVALUATION OF EOI

1. The EOIs received by the designated date and time will be examined by SEBI to determine if they meet the terms and conditions mentioned in this document including its subsequent amendment(s), if any and whether EOIs are complete in all respects.

2. On scrutiny, the EOIs found NOT in desired format/illegible/incomplete/not containing clear information, will be rejected for further evaluation process.

3. If deemed necessary, SEBI may seek clarifications on any aspect of EOI from the applicant. If a written response is requested, it must be provided within 3 days. Response received beyond 3 days, if any, will not be considered. However, that would not entitle the applicant to change or cause any change in the substances of their EOI document already submitted. SEBI will also make enquiries to establish the past performance of the applicants in respect of similar work. All information submitted in the application or obtained subsequently will be treated as confidential.

SN	**Criteria**	**Marks**	**Documents Required**	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
1.	Past experience of the bidder in Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification (track record)	75		
A	Number of year's relevant experience (IT Policy preparation or IT Risk Assessment or IT SOP documentation or process design specification. At least one project should be done in each section to get marks for this sub-criterion. The earliest		5	1. Copy of Purchase Order. 2. Self-declaration by the bidders declaring completion of the project or currently it is an on-going project.

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	PO out of the four sections will be considered for assigning marks.) More than 5 years – 5 marks ≥1 year and ≤ 5 years – 4 marks			

B	Past Experience in carrying out projects in Banking / Financial, Critical Infrastructure Institutions and/or private business units (IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification). >5 POs – 15 marks ≤5 POs and ≥ 4 POs - 14 marks ≤ 3 POS and ≥ 1 PO - 12 marks		15	1. As per format enclosed at Annexure IV. 2. Copy of Purchase Order. 3. Self-declaration by the bidders declaring completion of the project or currently it is an on-going project. The submitted projects can be of following types: Scope of Work (SOW) sections (Policy preparation, Risk Assessment, SOP documentation, Process Design Specification) All four SOW sections in single PO **OR** Any three SOW section in one PO and remaining one SOW section in another PO **OR** Any two SOW section in one PO and remaining two SOW section in another PO **OR** All four SOW section in four different PO

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
C	CERT-In Empanelment for last 3 consecutive years as on date of EOI.		3	Proof of CERT-In empanelment for last 3 consecutive years as on date of EOI.
D	i. Submit framework and scorecard for effective implementation of policies, SOPs and its automation. Such matrix should contain quantitative and qualitative representation and turnaround time for policy implementation so that SEBI will use such matrix in future to evaluate the SOP prepared. The policy should contain framework for implementation. SOP and automated section should contain a scorecard for evaluation and proof of evidence for every compliance point of policy. ii. Submit sample risk assessment framework.		24	i. Framework and scorecard for any one of the following (18 marks): 1. Disaster Recovery and BCP Policy 2. Incident Management Policy 3. Patch Management Policy ii. Risk Assessment framework (6 marks).

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	Bidder is required to give presentation of the framework, scorecard and risk assessment framework submitted under this sub-criterion. The framework and scorecard shall take example of either Disaster Recovery and BCP Policy or Incident Management Policy or Patch Management Policy to demonstrate the templates.			
E	Submit risk assessment report, best 3 policies, SOPs and design specification documents for automation done through projects of similar nature IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification) and implemented for the customer along with the details. If non-disclosure agreement was signed by the bidder, then they may submit examples of		24	Policy, SOP and design specification document, risk assessment report and Copy of Purchase Orders.

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	such work without disclosing exact customer name. Bidder is required to give presentation of the policies and risk assessment details submitted under this sub-criteria.			
F	Submit 2 PO documents and confirmation of certification from customer where bidder prepared policy documents aligned with ISO standards and ISO certification was successfully done through them. 2 marks for each PO with certification confirmation letter from customer.		4	Copy of Purchase Orders and confirmation of certification from customer or copy of ISO certificate.
2.	General profile of qualification, experience, and number of key professionals	13		
A	Qualifications.		7	1. Certificate from HR that these resources with

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	Certified professionals – No of ITIL / IT security / CISA / CISSP / CISM / CRISC certified professionals. > 12 professionals – 7 marks ≥ 8 and ≤ 12 professionals – 6 marks < 8 professionals – 0 marks			required qualifications are on full time rolls of the Bidder. 2. Copy of certificates.
B	Relevant experience. Average relevant experience of resources who have handled IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification projects. ≥ 5 years – 6 marks ≥4 years and <5 years – 5 marks ≥3 years and <4 years – 4 marks ≥ 2 years and <3 years – 3 marks Less than 2 years – 0 marks		6	Certificate from HR that the these resources with relevant experience are on full time rolls of the Bidder.
3.	Overall strength of the bidder in terms of	12		

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	turnover and profitability.			
A	The Average Annual Turnover figure for last three years via IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification and Security testing. For last three financial years ending on 31st March, 2020. If turnover is ≥ 70 Lakhs – 6 marks. If turnover is ≥ 60 Lakhs and < 70 Lakhs – 4.5 marks. If turnover is > 0 and < 60 Lakhs – 0 marks.		6	Self-declaration from the company signed by company's authorized signatory. 2019 – 2020 2018 – 2019 2017 – 2018
B	Net profit figure for last three years. For last three financial years ending on 31st March, 2020. If net profit is ≥ 20 lakhs– 6 marks		6	

SN	Criteria	Marks	Documents Required	
	Sub- Criteria	**Criteria Total marks**	**Sub-Criteria**	
	If net profit is ≥ 12 lakhs and <20 Lakhs– 4.5 marks If net profit is > 0 and < 12 Lakhs – 0 marks The bidder should not have suffered any financial loss for more than one year during the last three years, ending previous financial year.			
	Total	**100**		

4. Bidders (who have not been rejected in earlier steps) would be shortlisted based on the evaluation criteria as given in the above table.

1. The Bidders scoring marks 75 or above will be ranked based on their scores.

2. SEBI reserves the right to contact the reference clients to ascertain the submission made by the bidders, during the evaluation process.

3. The criteria Past experience and Financial strength, as mentioned above, will be relaxed for Startups[1] as follows –

[1] As defined by Department of Industrial Policy & Promotion (DIPP) an entity shall be considered as a 'start-up'-
a) Up to ten years from the date of its incorporation/registration,
b) If its turnover for any of the financial years has not exceeded INR 100 (Rupees One Hundred) crore
c) It is working towards innovation, development, deployment or commercialization of new products, processes or services driven by technology or intellectual property;
d) Provided further that in order to obtain benefits a start-up so identified under the above definition shall be required to obtain a certificate of an eligible business from the Inter-Ministerial Board of Certification.

SN	Criteria	Relaxation
1	Past experience of the bidder (track record)	A. Number of year's relevant experience (IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification. At least one project should be done in each section to get marks for this sub-criterion. The earliest PO out of the three sections will be considered for assigning marks). For Startups: More than 3 years – 5 marks ≥1 year and ≤ 3 years – 4 marks B. Past Experience in carrying out projects in Banking/ Financial, Critical Infrastructure Institutions and/or private business units (IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification)[2]: >3 POs – 15 marks ≤3 POs and ≥ 1 PO - 12 marks The submitted projects can be of following types: Scope of Work (SOW) sections (Policy preparation, Risk Assessment, SOP documentation) All four SOW sections in single PO **OR**

[2] The bidder references should contain large scale and related projects only, along with the requested details. If the project information submitted by the bidder is not relevant or is incomplete, SEBI may not consider it as valid experience and the decision of SEBI in this regard will be final.

SN	Criteria	Relaxation
		Any three SOW section n in one PO and remaining one SOW section in another PO **OR** Any two SOW section in one PO and remaining two SOW section in another PO **OR** All four SOW section in four different PO. Sub-criteria 1 (C) to 1 (F) remains same for Startups.
2	Overall financial strength of the bidder in terms of turnover and profitability.	For last three financial years ending on 31st March, 2020. 2019 – 2020 2018 – 2019 2017 – 2018 If turnover is ≥ 50 Lakhs– 6 marks If turnover is ≥ 45 Lakhs and < 50 Lakhs– 4.5 marks If turnover is > 0 and < 45 Lakhs – 0 marks If net profit is ≥ 15 lakhs– 6 marks If net profit is ≥ 9 lakhs and <15 Lakhs– 4.5 marks If net profit is > 0 and < 9 Lakhs – 0 marks The bidder should not have suffered any financial loss for more than one year during the last three years, ending previous financial year.

SECTION VIII – TERMS & CONDITIONS

1. Submission of an EOI is evidence of a Bidder's consent to comply with the terms and condition of Request for EOI process and subsequent bidding process. If a Bidder fails to comply with any of the terms, its bid may be summarily rejected.

2. Willful misrepresentation of any fact in the EOI will lead to the disqualification of the Bidder without prejudice to other actions that SEBI may take. The EOI and the accompanying documents will become property of SEBI. The Bidders shall be deemed to license, and grant all rights to SEBI, to reproduce the whole or any portion of their product/solution for the purpose of evaluation, to disclose the contents of submission to other Bidders and to disclose and/ or use the contents of submission as the basis for EOI process.

3. SEBI reserves the right to accept or reject any or all EOIs received without assigning any reason whatsoever and SEBI's decision in this regard will be final.

4. SEBI reserves the right to inspect the facilities of the bidder any time during the evaluation stage to verify the genuineness and to ensure the conformity with the proposal submitted.

5. The bidder is required to submit its full profile giving details about organization, experience, technical personnel in the organization, competence and adequate evidence of its financial standing etc. in the enclosed form which will be kept confidential.

6. No contractual obligation whatsoever shall arise from the EOI process.

7. Any effort on the part of Bidder to influence evaluation process may result in rejection of the EOI.

8. SEBI is not responsible for non-receipt of EOIs within the specified date and time due to any reason including postal delays or holidays in between.

9. SEBI reserves the right to verify the validity of information provided in the EOIs and to reject any bid where the contents appear to be incorrect, inaccurate or inappropriate at any time during the process of EOI.

10. Bidders shall be deemed to have:

    a. Examined the Request for EOI document and its subsequent changes, if any for the purpose of responding to it.

b. Examined all circumstances and contingencies, having an effect on their EOI application and which is obtainable by the making of reasonable enquiries.
c. Satisfied themselves as to the correctness and sufficiency of their EOI applications and if any discrepancy, error or omission is noticed in the EOI, the Bidder shall notify SEBI in writing on or before the end date/time.

11. The bidder shall bear all costs associated with submission of EOI, presentation/POC desired by SEBI. SEBI will not be responsible or liable for any cost thereof, regardless of the conduct or outcome of the process.

12. Bidders must advise SEBI immediately in writing of any material change to the information contained in the EOI application, including any substantial change in their ownership or their financial or technical capacity. Copies of relevant documents must be submitted with their advices.

13. Shortlisted Bidders must not advertise/publicize in any form (without prior written permission from SEBI) about their unit having been shortlisted by SEBI.

14. The detailed scope of work will be included in the Request for Proposal (RFP) document which shall be issued to all the qualified bidders. Technical evaluation of the submitted bids with respect to the RFP will then be evaluated. Technically qualified bidders will be selected under L1 criterion. Financial bid will be evaluated only for the technically qualified bidders.

15. SEBI may re-visit any of the conditions of this EOI, before the deadline for submission.

16. SEBI shall have the right to cancel the tendering process at any time, without thereby incurring any liabilities to the affected Bidders. Reasons for cancellation, as determined by SEBI in its sole discretion include but are not limited to, the following:

    a. Services contemplated are no longer required
    b. Scope of work not adequately or clearly defined due to unforeseen circumstance and/or factors and/or new developments
    c. The project is not in the best interest of SEBI
    d. Any other reason

17. The project engagement period for IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification project is for three years with details as follows:

First Year	a) In-depth risk assessment of IT infrastructure deployment at SEBI. b) Calculate risk score. c) Propose controls for vulnerability and threats; Control recommendations. d) Submit all reports related to risk assessment
	a) Phase I – Identify first 25-30 critical policies, dependent policies and SOPs. b) Prepare/review phase – I policies and SOPs in SEBI. c) Develop design specification for each process and sub-process identified in phase – I. d) Submit all the required policies, project wise plans, guidelines, SOPs and design specifications as per phase – I. e) Phase – II - Identify next 25-30 policies, dependent policies and SOPs. f) Prepare/review phase – II policies and SOPs in SEBI. g) Develop design specification for each process and sub-process identified in phase – II. h) Submit all the required policies, project wise plans, guidelines, SOPs and design specifications as per phase – II.
Second Year	a) Risk Assessment of IT infrastructure deployment at SEBI b) Calculate risk score. c) Propose controls for vulnerability and threats; Control recommendations. d) Submit changes required in the reports related to risk assessment.
	a) Phase III – Identify next 25-30 critical policies, dependent policies and SOPs. b) Prepare/review phase – III policies and SOPs in SEBI. c) Develop design specification for each process and sub-process identified in phase – III. d) Submit all the required policies, project wise plans, guidelines, SOPs and design specifications as per phase – III. e) Phase – IV - Remaining policies, dependent policies and SOPs. f) Prepare/review phase – IV policies and SOPs in SEBI. g) Develop design specification for each process and sub-process identified in phase – IV. h) Submit all the required policies, project wise plans, guidelines, SOPs and design specifications as per phase – IV .

Third Year	a) Risk Assessment of IT infrastructure deployment at SEBI b) Calculate risk score c) Propose controls for vulnerability and threats; Control recommendations. d) Submit changes required in the reports related to risk assessment

ANNEXURE I - ELIGIBILITY CRITERIA

< Name of the Bidder >

IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification

SN	Eligibility Criteria	Compliance (Yes/No)	Bidder's Response	Attachment Tag/ Page No.
1	• The bidder should be registered as a company in India as per Company Act 1956/2013 or a partnership firm registered under LLP Act, 2008 • Should have operation for a period of at least 3 years as on date of EOI.			
2	The bidder should have registered office in India. Also bidder should have office in Mumbai Metropolitan Region from where this project will be executed.			
3	The bidder should fulfill one of the following criteria in respect of past experience of having successfully completed similar projects over the last five years i.e. current financial year and the last five financial years: Three similar completed projects costing not less than the amount equal to INR 78,20,000/- (Seventy-Eight Lakhs Twenty Thousand only) OR Two similar completed projects costing not less than the amount equal to INR 97,75,000/- (Ninety-			

	Seven Lakhs Seventy-Five Thousand only) OR One similar completed project costing not less than the amount equal to INR 1,56,40,000/- (One Crore Fifty-Six Lakhs Forty Thousand only).			
4	The bidder should not be a blacklisted firm/company in any Govt. department/Banks/ PSU/other institution in India due to unsatisfactory performance, breach of general or specific instructions, corrupt or fraudulent or any other unethical business practices.			
5	In order to avoid conflict of interest, bidder must not be the existing application implementer(s) and / or solution provider(s) of SEBI.			

ANNEXURE II - EOI SUBMISSION FORM

(To be submitted on the letter head of the Agency(s))

Date: _____

To,
Shri Manojan Karayi
Chief General Manager,
Information Technology Department,
Securities and Exchange Board of India
SEBI Bhavan – II, Plot no C7,
G-Block, Bandra-Kurla Complex,
Bandra (E), Mumbai-400 051

Dear Sir,

Subject: Submission of the Expression of Interest (EOI) for **Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification**

We, the undersigned, offer to provide services for "*Information Technology Risk Assessment, Policy & SOP documentation and Process Design Specification*" to SEBI in accordance with your Expression of Interest (EOI) for **Information Technology Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification** dated December 15, 2020. We are hereby submitting our Expression of Interest (EOI).

We hereby declare that all the information and statements made in this Expression of Interest (EOI) are true and accept that any misinterpretation contained in it may lead to our disqualification.

We agree to abide by all the terms and conditions of the EOI document. We understand you are not bound to accept any proposal you receive.

Yours sincerely,

Authorized Signature [In full and initials]: _____

Name and Title of Signatory: _____

Name of Bidder: _____

Address: _____

Location: _____ Date: _____

ANNEXURE III – BIDDER'S INFORMATION DETAILS

Sr. No.	Items	Bidder's Response
1	**Basic Information**	
	a) Name of the organization	
	b) Name of the contact person	
	c) Registered office Address	
	d) Phone no. of the contact person	
	e) Email address of the contact person	
	f) Web site if any, of the organization	
	g) Year of commencement of business	
	h) PAN no.	
	i) Service tax registration No. / GST No.	
2	Location of competency center and number of professionals	
3	Number of years of relevant experience in IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification	
4	Past Experience in carrying out projects in Banking / Financial, Critical Infrastructure Institutions and/or private business units (IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification)– No of projects	
5	CERT-In Empanelment for last 3 consecutive years as on date of EOI.	
6.i	Framework and scorecard for effective implementation of policies, SOPs and its automation. Such matrix should contain quantitative and qualitative representation and turnaround time for policy implementation so that SEBI will use such	

	matrix in future to evaluate the SOP prepared. The policy should contain framework for implementation. SOP and automated section should contain a scorecard for evaluation and proof of evidence for every compliance point of policy. The framework and scorecard shall take example of either Disaster Recovery and BCP Policy or Incident Management Policy or Patch Management Policy to demonstrate the templates.	
6.ii	Sample risk assessment framework.	
7	Risk assessment report, best 3 policies, SOPs and design specification documents for automation done through projects of similar nature (IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification) and implemented for the customer along with the details. If non-disclosure agreement was signed by the bidder, then they may submit examples of such work without disclosing exact customer name.	
8	Purchase/Work Order documents and confirmation of certification from customer where bidder prepared policy documents aligned with ISO standards and ISO certification was successfully done through them.	
9	Qualifications Certified professionals – No of ITIL / IT security / CISA / CISSP / CISM / CRISC certified professionals	
10	Relevant experience Average relevant experience of resources who have handled IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification projects	

11	*Annual turnover of the bidder (in Rupee Lakhs) in last 3 financial years via* IT Risk Assessment, Policy & SOP Documentation and Preparing Process Design Specification *and Security testing.*	
	For 2019-20	
	For 2018-19	
	For 2017-18	
12	*Net profits during past three financial years Net Profit (In Rupee Lakhs):*	
	For 2019-20	
	For 2018-19	
	For 2017-18	
13	When applying as 'Startups' - Certificate of an eligible business from the Inter-Ministerial Board of Certification	

Authorized Signatory:

Name of the Authorized Signatory: Date:

Place: Seal:

ANNEXURE IV- PROJECT DETAILS

Details of project undertaken in financial institution/ Stock Exchange/ Regulatory authority in India or internationally (Attach Copy of Purchase orders/ any documentary evidence) (One sheet for each Project should be submitted)

Project no. 1 ….

SN	Items	Mandatory (Y/N)	Bidder's Response
1	Name of the project	Y	
2	Client name		
3	Location of client along with contact person, contact no and email id	Y	
4	a. Date of Purchase Order received for the project b. Date of Commencement of Contract: c. Date of Implementation of the project: d. Status of the Project (whether Completed / Work-in-progress etc.):	Y	
5	Nature of project for the Clients (Please list the activities handled by the bidder)	Y	
6	Scope of Work	Y	
7	Team Size	Y	
8	Name of the Project Head	Y	
9	Name of the Expert / Expert Team members	Y	
10	Software Tools & Technology used	Y	
11	Total Efforts in Man months	Y	
12	Contract Amount (in Rupees Lakhs)	N	
13	Any other relevant information including reason for delay if any	N	

Note: The bidder should give the above information in this format only.

Authorized Signatory:

Name of the Authorized Signatory: Date:

Place: Seal:

ANNEXURE V- ESTIMATED COST

SN	Component	Duration	Estimate Cost
1	Risk Assessment	First Year budget estimate	
		Second Year budget estimate	
		Third Year budget estimate	
2	Policy documentation	Four Phases of 6 months each	
3	Standard Operating Procedure documentation		
4	Design Specification for Process Automation		
	Total Cost		

ANNEXURE VI- CHECKLIST

Check list of enclosure:		
1	All supporting documents required in SECTION V Bidder's Eligibility Criteria	YES/NO
2	Annexure-I attached	YES/NO
3	Annexure-II attached	YES/NO
4	Annexure-III attached	YES/NO
5	Annexure-IV attached	YES/NO
6	Annexure –V attached	YES/NO
7	Annexure –VI attached	YES/NO
8	Any other (Please Specify)	YES/NO

ANNEXURE VII- Details of SEBI Custom Applications for Budget Estimate

SN	Application	User Department	Technology Used
1	SEBI Website	Whole SEBI & external users	Java, IBM Business Process Management, DB2, MS-SQL, SAS, Business Intelligent tools, ERP – SAP, IBM Analytical software, etc.
2	Investor Website	Department for Investor Assistance & External users	
3	Application 1	Market Intermediaries Regulation & Supervision Department for Primary and Secondary Market	
4	Application 2	Department for Investor Assistance & External users	
5	Application 3	Department for Legal Affairs	
6	Application 4	Analytical tool used by Surveillance Department	
7	Application 5	Internal Application being used by Investigation Department	
8	Application 6	Internal Application being used by Surveillance Department	
9	Email	Used by whole SEBI	
10	Infrastructure		Network devices, IP Telephony, Desktops, Laptops, Video Conferencing

SN	Application	User Department	Technology Used
11	Portal	Used by whole SEBI	Internal applications and External applications
12	SEBI Private Cloud	Implementation on going	

- Note- This list is an indicative list only.