



Unique Identification Authority of India (UIDAI)

Planning Commission, Government of India

REQUEST FOR PROPOSAL (RFP)

**“Hiring of Services for design and implementation of the GRC
Framework and providing Performance Assurance Services for UIDAI”**

Section V- Terms of Reference

PART 1: INTRODUCTION	4
1. ABOUT UIDAI	4
2. ABOUT AADHAAR.....	4
2.1.AADHAAR AUTHENTICATION	4
2.2.GOALS AND EXPECTED BENEFITS OF AADHAAR	5
2.3.STRATEGIC THINKING	6
2.4.FEATURES OF THE UIDAI MODEL	6
2.5.ENROLMENT AND AUTHENTICATION PLAN.....	8
3. THE UIDAI SERVICE DELIVERY FRAMEWORK.....	9
4. UIDAI ECOSYSTEM PARTNERS.....	10
5. UIDAI BUSINESS PROCESSES.....	17
5.1ENROLMENT	17
5.2.AUTHENTICATION.....	18
5.3.AADHAAR ENABLED ACCOUNT	20
5.4.AADHAAR ENABLED PAYMENT	21
5.5.UPDATION	23
5.6.REPORTING (BI AND PORTAL).....	23
6. UIDAI INFRASTRUCTURE	23
6.1.PHYSICAL INFRASTRUCTURE.....	23
7. UNDERSTANDING THE UID TECHNOLOGY SOLUTION	24
7.1.UID-TECHNOLOGY SOLUTION ARCHITECTURE DEVELOPMENT	24
7.2.UID SYSTEM FUNCTIONAL OVERVIEW.....	25
7.3.STRUCTURE OF UID TECHNOLOGY SOLUTION.....	26
7.4.UID SYSTEM OVERVIEW.....	27
7.5.INFORMATION SECURITY	42
PART 2: GOVERNANCE, RISK, COMPLIANCE FRAMEWORK AND PERFORMANCE	
ASSURANCE SERVICES	47
8. NEED AND OBJECTIVE OF IT SECURITY GOVERNANCE, RISK, COMPLIANCE AND	
PERFORMANCE ASSURANCE (GRCP).....	47
9. AADHAAR - GOVERNANCE, RISK, COMPLIANCE AND PERFORMANCE ASSURANCE	
(GRCP) FRAMEWORK	48
10. SCOPE FOR GRCP-SP	55
10.1GOVERNANCE	56
10.2.RISK.....	63

10.3.COMPLIANCE	71
10.4.PERFORMANCE.....	103
10.5.TECHNOLOGY REFRESH	104
10.6.EXIT / TRANSITION MANAGEMENT.....	106
10.7.SUMMARY OF LIST OF DELIVERABLES	109
10.8.ROLES AND RESPONSIBILITIES OF UIDAI:.....	122
11. IMPLEMENTATION SCHEDULE.....	124
12. BILL OF MATERIAL.....	126
12.1.LOG, NETWORK ANALYSIS.....	130
12.2.NETWORK SECURITY ANALYTICS	134
12.3.MALWARE ANALYSIS	137
12.4.FORENSICS	139
12.5.GRC.....	146
12.6.FRAUD DETECTION	161
12.7.RISK SIMULATION	162
12.8.INDOOR LED VIDEO WALL SPECIFICATIONS:.....	163
12.9.ADDITIONAL COMPONENTS TO BE BROUGHT IN BY GRCP-SP FOR STARMC:.....	164
13. KEY PERSONNEL	165

SECTION V: TERMS OF REFERENCE

Part 1: Introduction

1. About UIDAI

The Unique Identification Authority of India (UIDAI) has been created by the Government of India as an attached office under the Planning Commission. Its role is to develop and implement the necessary institutional, technical and legal infrastructure to issue Unique identity numbers to Indian residents. The Unique ID project is expected to lay the foundation for all future e-Governance projects in India in the coming decades. It is with this background that India's Unique ID initiative has been christened as "Aadhaar" (a Hindi word meaning "foundation").

2. About Aadhaar

Aadhaar is a 12-digit unique number which the Unique Identification Authority of India (UIDAI) will issue for all residents. The number will be stored in a centralized database and linked to the basic demographics and biometric information – photograph, ten fingerprints and iris – of each individual. Unique features of Aadhaar-based identifications are as follows:

- a. Universality, which is ensured because Aadhaar will, over time be recognized and accepted across the country and across all service providers.
- b. Every resident's entitlement to the number.
- c. The number will consequently form the basic, universal identity infrastructure over which Registrars and Agencies across the country can build their identity-based applications.

Note: In all the documentation provided as part of this ToR, the terms UID, Unique ID and Aadhaar are used synonymously.

2.1. Aadhaar Authentication

Aadhaar authentication is the process wherein Aadhaar number, along with other attributes (demographic/biometrics/OTP) is submitted to UIDAI's Central Identities Data Repository (CIDR) for verification; the CIDR verifies whether the data submitted matches the data available in CIDR and responds with a "yes/no". No personal identity information is returned as part of the response.

The purpose of Authentication is to enable residents to prove their identity and for service providers to confirm that the residents are 'who they say they are' in order to supply services and give access to benefits.

2.2. Goals and expected benefits of Aadhaar

It is expected that this Aadhaar ecosystem will deliver the following benefits to residents of India:

- i. Aadhaar will ensure increased trust between public and private agencies and residents. Once residents enroll for Aadhaar, service providers will no longer face the problem of performing repeated Know Your Customer (KYC) checks before providing services. Residents would also be spared the trouble of repeatedly proving identity through documents each time they wish to access services such as obtaining a bank account, passport, or driving license etc.
- ii. By providing a clear proof of identity, Aadhaar will empower poor and underprivileged residents in accessing services such as the formal banking system and give them the opportunity to easily avail various other services provided by the Government and the private sector.
- iii. The centralized technology infrastructure of the UIDAI will enable 'anytime, anywhere' authentication. Aadhaar will thus give migrants mobility of identity.
- iv. Aadhaar authentication can be done both offline and online, online authentication through a cell phone or land line connection will allow residents to verify their identity remotely.
- v. Remotely, online Aadhaar-linked identity verification will give poor and rural residents the same flexibility that urban non-poor residents presently have in verifying their identity and accessing services such as banking and retail.
- vi. Aadhaar will also demand proper verification prior to enrolment, while ensuring inclusion. Existing identity databases in India are fraught with problems of fraud and duplicate or ghost beneficiaries. To prevent these problems from seeping into the Aadhaar database, the UIDAI plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean from the beginning of the program.
- vii. Much of the poor and under-privileged population lack identity documents and Aadhaar may be the first form of identification they will have access to. The UIDAI will ensure that its 'Know Your Resident (KYR)' standards do not become a barrier for enrolling the poor and has accordingly developed an Introducer system for residents who lack documentation. Through this system, authorized individuals ('Introducers') who already have an Aadhaar, can introduce residents who don't have any identification documents, enabling them to receive their Aadhaar.

2.3. Strategic Thinking

The strategic goals of UIDAI Program are:

- i. Inclusion of poor people
 - a. The UIDAI envisions full enrolment of the residents, with a focus on enrolling India's poor and underprivileged communities. It is proposed to enroll 600 million people over next 4 years.
- ii. Social Benefits
 - a. Reducing leakage in government social expenditure through de-duplication of beneficiary lists
 - b. Enabling Financial Inclusion by Aadhaar Enabled payment system
 - c. Enabling direct delivery of benefits to the resident by Aadhaar payment bridge
- iii. Technology Benefits to the Government sector
 - a. Create an e-governance cloud platform to be shared by central and state governments
 - b. Ready to use platforms, easy to build applications with reusable technology elements and components, processes and skills
 - c. No headache for every government agency to build, commission and operate its own platform
 - d. Provide a boost to relevant technology, including biometrics
 - e. Increase the amount of software in the public domain / open source.
 - f. Rapid implementation of e-governance initiatives
- iv. Benefits to Organizations
 - a. Enable organizations to create a single customer master
 - b. A platform for low cost authentication

For details on the goals of UID system, refer to the document on UIDAI's website titled "Creating a unique identity for every resident in India - Draft approach".

2.4. Features of the UIDAI Model

- i. **The UID number will only provide identity:** The UIDAI's purview will be limited to the issue of unique identification numbers linked to a person's demographic and biometric information. The UID number will only guarantee identity, not rights, benefits or entitlements.
- ii. **The UID will prove identity, not citizenship:** All residents in the country can be issued a unique ID. The UID is proof of identity, and does not confer citizenship.
- iii. **A pro-poor approach:** The UIDAI envisions full enrolment of the residents, with a focus on enrolling India's poor and underprivileged communities. The Registrars

- that the Authority plans to partner with in its first phase – the NREGA, RSBY, and PDS – will help bring large numbers of the poor and underprivileged into the UID system. The UID method of authentication will also improve service delivery for the poor.
- iv. **Enrolment of residents with proper verification:** Existing identity databases in India are fraught with problems of fraud and duplicate / ghost beneficiaries. To prevent this from seeping into the UIDAI database, the Authority plans to enrol residents into its database with proper verification of their demographic and biometric information. This will ensure that the data collected is clean from the start of the program.
 - v. However, much of the poor and underserved population lack identity documents and the UID may be the first form of identification they have access to. The Authority will ensure that the Know Your Resident (KYR) standards don't become a barrier for enrolling the poor, and will devise suitable procedures to ensure their inclusion without compromising the integrity of the data.
 - vi. **A partnership model:** The UIDAI approach leverages the existing infrastructure of government and private agencies across India. The UIDAI will be the regulatory authority managing a Central ID Repository (CIDR), which will issue UID numbers, update resident information and authenticate the identity of the residents as required.
 - vii. In addition, the Authority will partner with agencies such as central and state departments and private sector agencies, who will be 'Registrars' for the UIDAI. Registrars will process UID applications, and connect to the CIDR to de-duplicate resident information, and receive UID number.
 - viii. **The UIDAI will emphasize a flexible model for Registrars:** The Registrars will retain significant flexibility in their processes, including issuing cards, pricing, expanding KYR verification, collecting demographic data on residents for their specific requirements, and in authentication. The UIDAI will provide standards to enable Registrars to maintain uniformity in collecting certain demographic and biometric information, and in basic KYR. These standards will be finalized by the KYR and biometric committees the Authority constitutes.
 - ix. **Process to ensure no duplicates:** Registrars will send the applicant's data to the CIDR for de-duplication. The CIDR will perform a search on key demographic fields and on the biometrics for each new enrolment, to minimize / eliminate duplicates in the database.
 - x. The incentives in the UID system are aligned towards a self-cleaning mechanism. The existing patchwork of multiple databases in India gives individuals the incentive to provide different personal information to different agencies. Since de-duplication in the UID system ensures that residents have a unique identify, it is expected that the individuals will provide accurate data. This incentive will become especially powerful as benefits and entitlements are linked to the UID.

- xii. **Online authentication:** The Authority will offer a strong form of online authentication, where agencies can compare demographic and biometric information of the resident with the record stored in the central database. The Authority will support Registrars and agencies in adopting the UID authentication process, and will help define the infrastructure and processes they need.
- xiii. **The UIDAI will not share resident data:** The Authority envisions a balance between ‘privacy and purpose’ when it comes to the information it collects on residents. The agencies may store the information of the residents they enroll if they are authorized to do so, but will not have access to the information in the UID databases. The UIDAI will answer all requests to authenticate identity only through a ‘Yes’ or ‘No’ response. The Authority will also enter into contracts with Registrars to ensure the confidentiality of the information they collect and store. In addition, internal stakeholders who may have role based access to resident data would be appropriately trained, sensitized and security cleared for handling such privacy related data.
- xiv. **Data Transparency:** The authority will publish all the aggregated data for the public to access under RTI. However, Personal Identity Information (PII) will NOT be accessible by any entity.
- xv. **Technology will undergird the UIDAI system:** Technology systems will have a major role across the UIDAI infrastructure. The UID database will be stored on a central server. Enrolment of the resident will be computerized, and information exchange between Registrars and the CIDR will be over a network. Authentication of the residents will be online. The MSP on behalf of the Authority will also put systems in place for the security and safety of information.

2.5. Enrolment and Authentication Plan

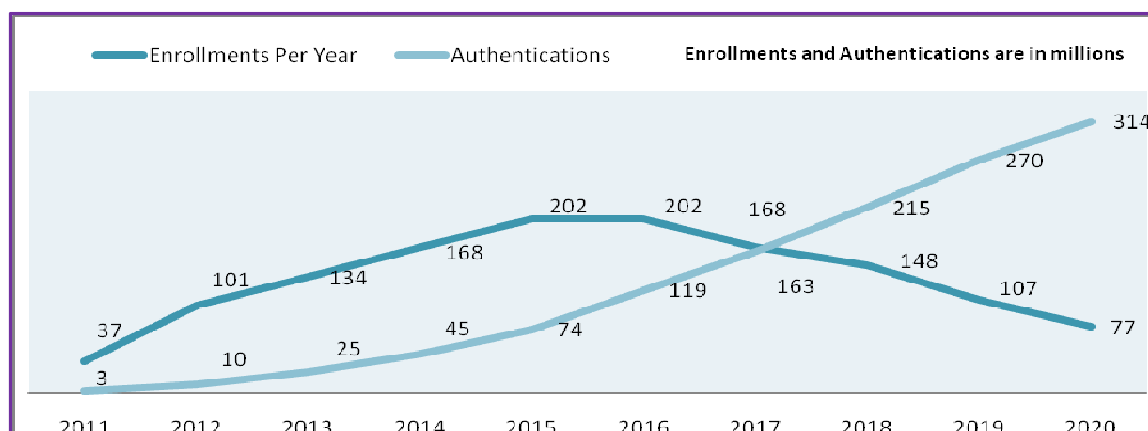


Figure 1: Expected Enrolment and Authentication Plan for Aadhaar

Note: Authentication transaction volumes in Figure 1 are estimated for Per Day. These are only indicative estimates. Actual numbers may vary.

- i. A predicted annual enrolment plan is shown in Figure 1. It is conceivable that the enrolments can happen more rapidly than shown above. As can be seen, a certain number of enrolments (200 million) need to be in the database before authentication (also known as verification) services can be meaningfully rolled out in.

3. The UIDAI Service Delivery Framework

- i. Serving the resident is the primary objective of the Aadhaar program. Both Government agencies as well as private sector will rely on the quality of services provided by Aadhaar to serve their customers in turn which are the Residents. From Resident's perspective, the key goals and objectives of UIDAI are:
 - a. Delivery of good quality services and
 - b. Guaranteed service delivery

Below is the illustrative framework which outlines the service delivery mechanism to ensure a seamless service delivery to citizens.

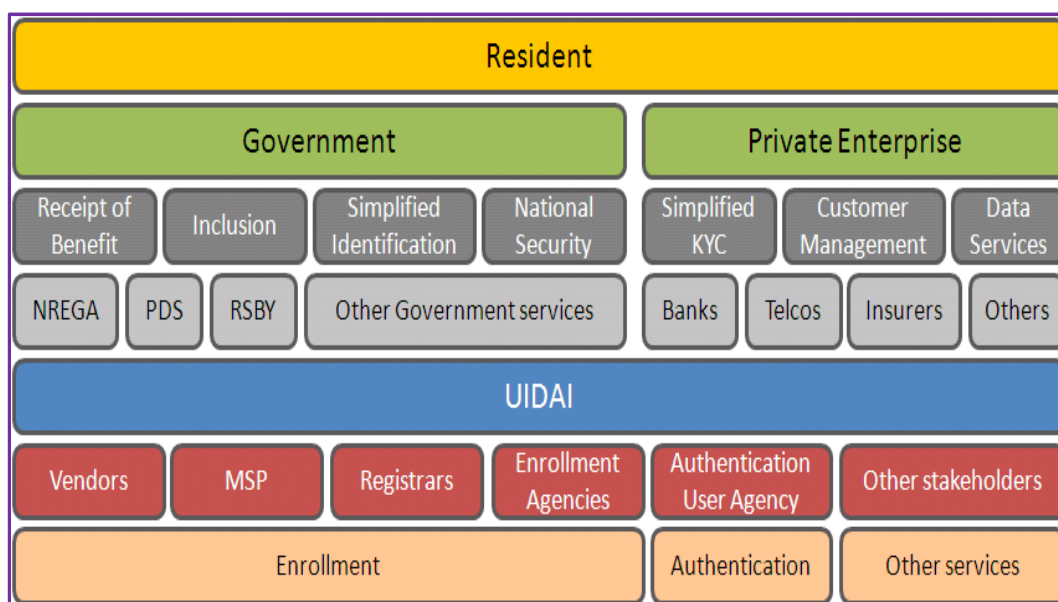


Figure 2: UIDAI Service Delivery Framework

4. UIDAI Ecosystem Partners

For delivery of good quality CIDR services through both government and private sector entities, UIDAI needs to create and manage a large ecosystem of agencies. This ecosystem will help in enrolment of residents and in delivery of authentication services which will help Government and Private Enterprise deliver services to the Resident. Various stakeholders and their respective roles are stated below:

- i. **UIDAI** – The Authority that will issue UID numbers and set standards for enrolment and authentication to be universally followed. Initially UIDAI will among other things design, develop, and deploy the UID Application with the help of service providers. Subsequently, the entire operations will be expanded and operated by an external service provider. In addition to providing the product and services, the UIDAI is responsible for appointing registrars, empanelling and approving enrolment agencies, providing a list of introducers among others. To further the mission, UIDAI will also help the creation of further services that depend on the UID authentication.
- ii. **Registrars** - These are public and private organizations who are currently engaged in providing services to the residents, and who operate on behalf of the UIDAI to provide UIDAI services (such as enrolment) to their constituents. Example profiles of registrars include state governments, ministries and departments in the central government, banks and other financial institutions, telephone companies, etc.
 - Registrars may collect documentation – such as proof of residence, and proof of identity from residents. Registrars are required to store such documents, and have them available for later investigation / audit.
 - Registrars may also receive some of the data collected as part of UID enrolment - specifically, they will have access to the demographic data, and photograph of the resident. Registrars may store the UID within their systems, as well as print it on artifacts provided to the resident (such as a card, or a letter). Certain registrars may store biometric data such as fingerprint, and IRIS in a secure manner on smart cards for offline authentication purposes. This data may not be stored on their servers, or used for online authentication.
 - To ease the process of registration for the marginalized, registrars may provide a list of introducers who may introduce residents (thus waiving certain proofs, as required by the KYR document). This list of introducers is Registrar specific.
 - Registrars are responsible to provide their own IT infrastructure including encryption and secure FTP and Standard operating environment as per guidelines by UIDAI

- Registrar Management includes,
 - a. Providing Training for performing enrolment and authentication services
 - b. Signing MOU with new public and private organizations
 - c. Providing System and Connectivity to perform enrolment and authentication services
 - d. Handling complaints from residents
 - e. Handling accounting and billing
- iii. **Enrolment Agency** - An agency contracted by the Registrar, subject to certification by the UIDAI, to perform their duties. Enrolment agencies provide operators, and supervisors for the enrolment stations on the field, and also create the necessary conditions for the optimal enrolment of residents. Enrolment agencies must collect demographic data prior to an enrolment drive. They must notify residents (and the UIDAI) of the enrolment schedule in advance. Enrolment agencies may be empanelled by the UIDAI. Enrolment Agencies are responsible to provide Biometric devices as per UIDAI specifications and certifications and follow standard operating procedures for enrolment and secure FTP as per guidelines by UIDAI. EAs are responsible to train their staff on security and privacy.
The enrolling agency is responsible for:
 - a. Procuring biometric devices as per UIDAI specifications
 - b. Setting up of enrolment stations and enrolment centres
 - c. Hiring and Training manpower for enrolment
 - d. Conduct enrolment operations as per standard processes specified by UIDAI
 - e. Send enrolment data to registrar
 - f. Ensure Security and Privacy of enrolment data
 - g. Provide electronic reports on enrolment status daily
- iv. **Introducer** - A well-known person authorized by the UIDAI or by a Registrar to introduce individuals to the UID. This mechanism was specifically created to allow the UID system to reach out to the marginalized and excluded residents who may not have sufficient documentation to meet the Proof of Identity or Address specified in the published KYR norms. Hence an introducer provides an assurance that the individual applying for a UID is indeed a resident, and to the best of his / her personal knowledge who they say they are. Registrars may provide a list of introducers with their name and UID to UIDAI.
- v. **Residents** - Residents of India, who wish to obtain a UID, are expected to provide appropriate documentation to meet the KYR norms, or to be introduced by an appointed introducer. A resident is defined as a natural person, usually residing in India. Residents are expected to truthfully provide information and documentation to meet the KYR norms, or be introduced by an introducer. Residents will have

access to their data, and the ability to identify when they were authenticated (for a period of time). Access to data of other residents is to be restricted by the UIDAI.

- vi. **Managed Service Provider** – It is proposed to either have a single entity called Managed Service Provider (“MSP”) or a group of entities (performing the roles of BSP, ASDMSA, DC operations, etc.) which shall collectively be referred to as MSP, to implement and manage the CIDR with the following broad roles and responsibilities:
- Installation, commission and manage the CIDR and undertakes data center operations for enrollment work and allotment of UID numbers.
 - Undertake the transition and transformation of the current UID programme for meeting the infrastructure needs of growing volume of enrollments.
 - Manage the existing contracts, SLAs and transition in a time-bound manner by maintaining the continuity of service level agreements.
 - Based on the macro level inputs from UIDAI on enrollment and authentication, undertake a modeling exercise by incorporating application level inputs and provision infrastructure augmentation and scaling of IT infrastructure.
 - Provide recommendations to the UIDAI and Architecture Review Board for technology refresh, and periodic augmentation of IT systems.
 - Assist the UIDAI agency in development of UIDAI ecosystems and undertakes development of third party applications for registrars or other stakeholders in the UIDAI ecosystem to reduce time to market.
 - Implement the recommendations of third party audits including system audit, security audit, network audit and SLA audit.
 - Manage the authentication part of the UIDAI programme and additional system integrators or managed service providers for authentication services at programme level.
 - Manage overall IT systems of CIDR and SLA and MIS reporting to the UIDAI agency.
 - Manage the enhancement, development and maintenance of the current UID Application (“UID-APP”) by bringing out next level version releases.
 - Manage the IT systems and other requirements of regional offices
- vii. **Application Software Development, Maintenance and Support Agency (ASDMSA)** – ASDMSA provides application software development and maintenance services for the UID application (“UID-APP”). Currently MindTree Ltd. is the appointed ASDMSA. In addition to development of the UID-APP, ASDMSA will also develop biometric based enrollment software and the biometric solution interface. Going forward, the MSP shall manage the enhancement, development and maintenance of the current UID Application (“UID-APP”) by bringing out next level version releases. This role of ASDMSA can be transferred to

another party(s) as per evolving business requirements of UIDAI. It is important for GRCP-SP to understand and cover ASDMSA as a role whether performed by one or multiple parties and should not be looked at as a function carried out by a particular entity.

viii. **Authentication User Agency**—An Authentication User Agency is an agency that uses the UID system to authenticate a resident. An AUA sends authentication requests to enable its services / business functions. An AUA connects to the CIDR through an ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA may use demographic data, and/or biometric data in addition to the resident's UID. AUA can be any government / public / private legal agency registered in India that seeks to use Aadhaar authentication for its services. Key AUA Responsibilities:

- Ensure compliance of authentication related operations (processes, technology, security, etc.) to UIDAI's standards and specifications.
- Prepare authentication packet as per Authentication API specifications.
- Log and maintain details of all authentication transactions.
- Ensure Best Finger Detection (BFD) application is implemented to on-board the residents for biometric authentication.
- Identifying exception-handling and back-up identity authentication mechanisms.
- Deploy fraud monitoring mechanism, to prevent misuse of exception handling mechanism by operators and any other ecosystem members.
- Get its operations and systems related to Aadhaar Authentication audited as per UIDAI's specifications.
- Ensure connectivity from authentication devices to the AUA server and between the AUA server and the ASA server.
- Procure, deploy and manage devices in compliance with UIDAI specifications.
- Ensure adequate training for the personnel managing authentication devices.
- Inform UIDAI of the engagement/ disengagement of Sub AUAs.
- Ensure supported Sub AUAs comply with UIDAI's standards and specifications.

Mandatory Security Requirements prescribed by UIDAI

- Aadhaar number should never be used as a domain specific identifier.
- In the case of operator assisted devices, operators should be authenticated using mechanisms such as password, Aadhaar authentication, etc.
- PID block captured for Aadhaar authentication should be encrypted during capture and should never be sent in the clear over a network.
- The encrypted PID block should not be stored unless it is for buffered authentication for a short period, currently configured as 24 hours.

- Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database.
 - The metadata and the responses should be logged for audit purposes.
 - Network between AUA and ASA should be secure.
- ix. **Authentication Service Agency (ASA)** - ASA is any entity that transmits authentication requests to the CIDR on behalf of one or more AUAs. They play the role of enabling intermediaries. They have an established secure connection with the CIDR and convey AUAs' authentication requests to the CIDR. ASAs receive CIDR's response and transmit the same back to the AUA. Key ASA Responsibilities:
- Ensure compliance of authentication related operations (processes, technology, security, etc.) to UIDAI's standards and specifications.
 - Log and maintain details of all authentication transactions.
 - Get its operations and systems related to Aadhaar Authentication audited as per UIDAI's specifications.
 - Perform basic checks on the authentication input and forward it to CIDR
 - Transmit the result of the authentication transaction received from CIDR to the AUA that has placed the request
 - Inform UIDAI of the engagement/ disengagement of AUAs that it serves
 - Inform UIDAI of any misuse of Aadhaar data, authentication services, or any compromise of Aadhaar related data or systems.
- Mandatory Security Requirements prescribed by UIDAI
- ASA can connect to the CIDR only through a secured leased line.
 - The metadata and the responses should be logged for audit purposes.
 - Encrypted PID block and license keys that come as part of authentication packet should never be stored anywhere in ASA's system.
 - Network between AUA and ASA should be secure.
- x. **Biometric Solution Provider (BSP)** – UIDAI has appointed three biometrics service providers. The biometric solution shall be used in the de-duplication in enrolments and for providing authentication services. Going forward, the BSP shall work under the direction of UIDAI and the Managed Service provider to supply, integrate, commission and manage biometric solutions.
- xi. **Data Center (DC) Service Provider** – The entire UID application, with the exception of the enrollment centers and authentication request stations, will be housed at co-located Data Centers initially at two physical centers, but potentially growing into multiple centers during the course of the project. UIDAI has appointed data centre service providers ("DCSP") to provide the collocated hosting services.

- xii. **Logistics Service Provider** - UID logistics services comprises of two components; namely - Inbound and Outbound logistics. UIDAI's goal for inbound logistics is to offer secure and quick transfer of demographic and biometric data collected by the enrolment agencies to the CIDR for the purpose of de-duplication and UID generation. UIDAI's goal for outbound logistics is to offer timely and secure delivery of the UID letter to the intended resident. The core logistics activities: printing, sorting, dispatching and delivery of the AADHAAR letter is currently handled by Department of Posts. The Managed Service Provider (MSP)/ agency appointed by UIDAI shall primarily be responsible for managing and monitoring the logistics provider as a part of logistics services functions being part of overall program management. The MSP for inbound logistics has the following responsibilities:
- Uploading of enrollment data from regional offices to CIDR network
 - Track and trace of all inbound data
 - Creating and maintaining necessary IT infrastructure and network equipment for inbound logistics
 - Check for completeness and correctness of content received

The Department of Posts in its role as Logistics Service Provider is as below:

- Sealing, encoding and dispatching memory stick as per UIDAI guidelines to CIDR.
- Sending electronic batch file of enrolments to CIDR.
- Timely and secure delivery of the envelope to intended residents.

MSP is responsible for measuring and monitoring the logistics process on a continuous basis. Any deviation from the expected levels of service in terms of quality and performance shall be reported to UIDAI periodically.

- xiii. **Contact Center Service Provider** - The Contact Center provides a central point of contact to residents and other entities that will partner with UIDAI during the enrolment and post enrolment stages. The Contact Center will provide services in multiple languages for residents, registrars, enrolment agencies and resident service agencies.
- xiv. **Device Certification Agency** - The devices used for Enrolment, Authentication, Micro-ATM and other UID functions should comply with the standards set by UIDAI. The Device Certification process includes,
- Devices used for enrolment and authentication are capable of delivering the outputs as specified by UIDAI
 - Ensuring devices are robust enough to be used in different climatic conditions
 - Check whether the device software has necessary application programming interfaces

- Ease of integration with demographic software used by UIDAI

The Standardization Testing and Quality Certification (STQC) have been selected as the Biometric Certification Agency for certifying biometric devices to comply with the standards set by UIDAI.

The device manufactures or suppliers who supply biometric devices for UID enrolment and authentication have to be certified by STQC and UIDAI. Please refer to the detailed Device Certification documents from UIDAI website.

- xv. **Testing and Certification Agencies** – Training and Certification agency is responsible for training the required workforce of Enrolment operators for executing UID enrolments in a time-bound fashion. They plan and formulate the overall Testing Plan, design the standard course-ware which can be used across the country for training of enrolment operators and conduct testing and certification to ensure quality of the trained personnel. This would involve developing and maintaining the IT infrastructure for test scheduling, test taker registration and online testing, setting up required test centers for conduct of online testing, and all other entailing administration responsibilities.
- xvi. **Training Agencies** - Persons involved in the enrolment process at the field level must be trained thoroughly to accomplish the job of enrolment. Similarly the supervisors of the enrolling agencies and the representatives of the Registrars who will be involved in the UID enrolment should also be sufficiently trained to ensure data-quality, especially of the biometric data which is the basis of de-duplication of biometric attributes of residents. As the number of enrolments is going to increase in the next few years, there will be a huge requirement of trained personnel.

The Training content includes,

- a. The UIDAI Eco-system
- b. The Key goals and objectives of Aadhaar
- c. The processes which need to be followed to ensure the success of Aadhaar initiative by UIDAI
- d. Understanding how to setup and manage an enrolment centre
- e. Handling of various types of devices which are required for enrolling residents
- f. Familiarization with the Aadhaar Enrolment Client which is used for entering data during the enrolment process
- g. Handling of exceptional cases during the enrolment process
- h. Handling residents, their concerns and objections

The UIDAI proposes to create an eco-system of training agencies and capacities in the country so as to provide manpower needed for enrolment. Currently, the selection for training agencies is in progress.

- xvii. **Aadhaar Empanelled Banks:** An Aadhaar empanelled bank is used to achieve the desired financial inclusion objective for founding the Aadhaar concept. They are responsible for creating a free ‘no-frills’ account called Aadhaar Enabled Account (AEBA) to the residents, linking the existing accounts with UID number, and offer them regular banking services thereafter as regulated by RBI regulations. During the time of enrolment, the resident can choose to create Aadhaar enabled account with an empanelled bank or Department of Posts. The empanelled bank has to receive data from UIDAI and set up the account in a fixed timeframe. The resident can later on convert the ‘no-frills’ account to normal savings account at the respective bank’s discretion.

5. UIDAI Business Processes

- i. In addition to looking at the entities, and their relationships it is important to understand the UIDAI business processes, and evaluate them for security threats. The key external facing business processes are highlighted here.
- ii. There are additional internal business processes, (which are standard for any IT enabled organization which are not documented here. For example, these include
 - a. Backups
 - b. System Administration
 - c. Disaster Recovery & Business Continuity Planning

However, these are considered, and included in the security architecture

5.1. Enrolment

- i. UIDAI enrolment is based on the collection of demographic and biometric data from a resident. This process is conducted by an enrolment agency on behalf of a particular registrar. The resident must be present in person, and provide existing proofs of identity, and address. The enrolment operator collects this information, captures biometrics, and provides the resident with an acknowledgement.
- ii. In addition to applying for a UID, the resident may have additional interactions with the agency for availing the registrar’s services. For instance, when the registrar is also responsible for the Public Distribution System, there could be interactions related to the ration Card.

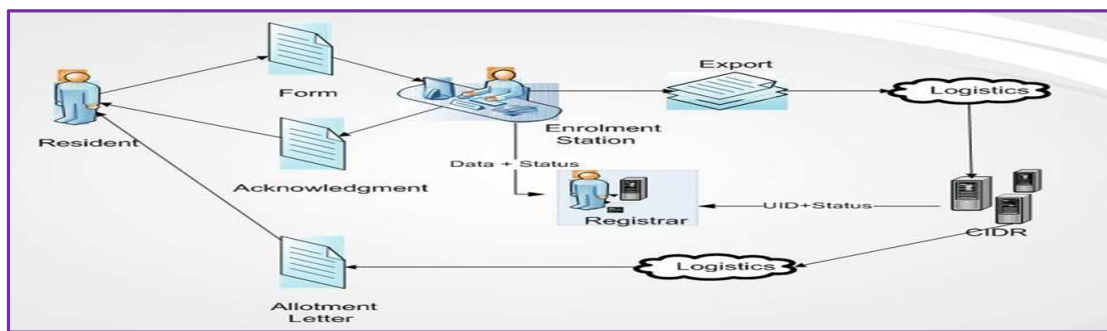


Figure 3: Enrolment at High Level

- iii. The collected data is sent to the CIDR for processing. The Aadhaarservers perform basic validation, and integrity checks on the received data to ensure that the data has not been tampered. The data is then validated; biometric enrolment is done to ensure that any resident gets only one Aadhaar Number. The Aadhaar Number is then generated, and a letter dispatched to the resident.
- iv. The enrolment process is conducted jointly with the registrar, and all data, including the allotted Aadhaarnumber is shared with the registrar.

5.2. Authentication

The authentication process involves interaction of many ecosystem partners such as Authentication User Agency, Authentication Service Agency, Sub-AUAs (the entity which desires to use Aadhaar authentication services but chooses to access this service by routing authenticationrequest through an existing AUA's infrastructure) with UIDAI's CIDR. Any agency that needs to authenticate residents for the purpose of service delivery could use Aadhaar authentication. Such an agency must register with the UIDAI as an Authentication User Agency. Authentication Service Agencies are entities that have secure leased line connectivity with the CIDR.

AUAs collect information required for Aadhaar authentication from the resident and transmit it to ASA. ASAs transmit authentication requests to CIDR on behalf of one or more AUAs. AUA's use Authentication devices to collect PID (Personal Identity Data) from Aadhaar holders.

The key partners could engage with each other in multiple ways. For example,

- An AUA could choose to become its own ASA, or
- An AUA could access Aadhaar authentication services through multiple ASAs for reasons such as business continuity planning or
- An AUA could transmit authentication requests for its own service delivery needs as well as on behalf of multiple Sub AUAs.

Similarly, it may also be possible to use a single authentication device for servicing multiple AUAs. For example, the authentication device at a fair price shop may also be used for carrying out financial transactions for banks.

Aadhaar number can be used for multiple types of authentication. The service delivery agencies select their appropriate authentication type based on their business requirements.

- i. Type 1 Authentication – Use Aadhaar Authentication system for matching Aadhaar number and the demographic attributes of a resident
- ii. Type 2 Authentication – Authenticate residents through One-Time-Password delivered to resident's mobile number and/or email address present in CIDR
- iii. Type 3 Authentication – Authenticate residents using one of the biometric modalities, either iris or fingerprint
- iv. Type 4 Authentication – This is a 2-factor authentication offering with OTP as one factor and biometrics (either iris or fingerprint) as the second factor for authenticating residents.
- v. Type 5 Authentication – Allows service delivery agencies to use OTP, fingerprint & iris together (3-factor authentication) for authenticating residents.

The Aadhaar number needs to be submitted in all forms of authentication so that this operation is reduced to a 1:1 match. Aadhaar number itself is not an authentication factor. Type 1 authentication may be combined with any other Aadhaar authentication offering.

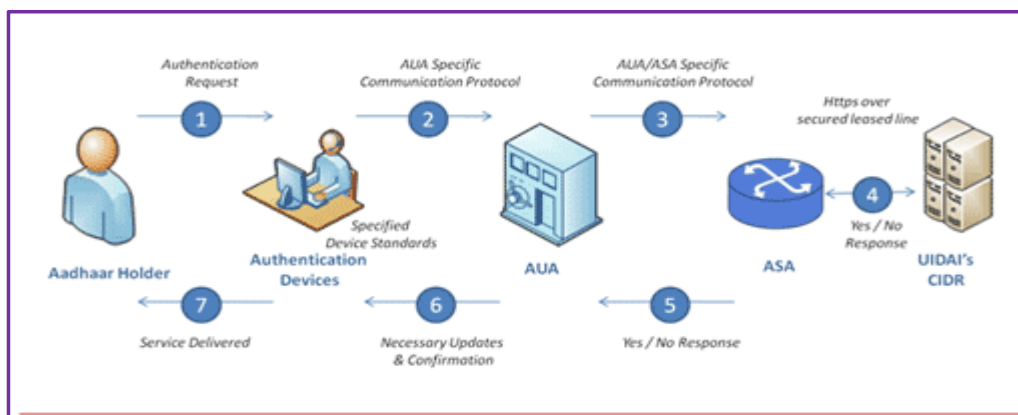


Figure 4: Authentication High Level View

The illustration above describes a typical authentication transaction.

- i. The Aadhaar Holder (Resident) approaches the local service provider for the purpose of obtaining a service. The local agency uses authentication devices that collect PID (Personal Identity Data), the Aadhaar number, and any additional

- demographic / biometric data required for the authentication. This is encrypted, and sent to the Authentication User Agency (AUA) back-office.
- ii. The Authentication User Agency transmits the authentication packets over a secured protocol to Authentication Service Agency (ASA).
 - iii. The Authentication Service Agency then interacts with the CIDR over a secured HTTPS leased line and transmits this information to CIDR for authentication purposes.

CIDR performs the authentication and the result of authentication travels back to the ASA and then to the AUA who then decides to deliver the requested service based on the authentication result. The sensitive data collected at the terminal is expected to be encrypted within the device itself, and may not be logged, or used for any other purposes. The CIDR is also expected to only log the data required for non-repudiation purposes. The tracking of residents and monitoring of their behaviour will not be possible at the CIDR.

For cases where connectivity is intermittent or connectivity is a little distance away leading to any network failure, UIDAI proposes a solution called “buffered” authentication wherein authentication request may be “buffered” (or queued) on the device until a pre-specified period of time, which is currently 24 hours, and then sent to CIDR for authentication when connectivity is restored / available. In addition, UIDAI expects that buffering would only be done at the device level and not at AUA / ASA server end. UIDAI is currently recommending procedures to AUAs for handling biometric exceptions.

For further details about authentication and related ecosystem partners, please refer to the Authentication section on UIDAI’s website.

5.3. Aadhaar Enabled Account

The UIDAI aims to empower the common man by providing a robust authentication infrastructure. This infrastructure is expected to facilitate access to a modern banking and payment systems. The goal of linking Aadhaar to an electronic bank account will empower the residents, particularly the marginalized, promote Electronic Benefit Transfers, induce business efficiencies and improve delivery of public services.

To achieve the objective of financial inclusion, it’s highly crucial to help the residents, especially the marginalized ones to facilitate in easy creation of accounts. For this purpose, UIDAI is the process of empanelling banks to initiate the creation of Aadhaarenabled accounts. An Aadhaar empanelled bank is used to achieve the desired financial inclusion objective for founding the Aadhaar concept. They are responsible for creating a free ‘no-frills’ account called Aadhaar Enabled Account (AEBA) to the residents, linking the existing accounts with UID number, and offer them regular banking services thereafter and regulated by RBI regulations .

Process flow for opening / linking bank accounts:

- During enrolment, Residents will also be asked to provide their consent for opening the bank account or linking their existing account in any one of the empanelled banks or Post Office Saving Bank (POSB)
- If the resident wants to link his/her existing bank account, then information with respect to his/her bank branch name, account number and IFSC code (if any) will also be collected from the resident.
- EA will send the KYR and biometric information along with EID of each resident to CIDR and subsequently after de-duplication, UIDAI will issue the Aadhaar letter to the resident.
- UIDAI will send the resident information to the bank chosen by the resident, for residents who have provided consent for opening/linking of bank account.
- Bank will communicate the bank account number to the resident after activating the account. An intimation of the same will also be sent to UIDAI through an established process.

5.4. Aadhaar Enabled Payment

To enable financial inclusion, UIDAI has partnered with various stakeholders including RBI, NPCI, IBA and banks to develop two key platforms:

- Aadhaar Payments Bridge (APB) – A system that facilitates seamless transfer of all welfare scheme payments to beneficiary residents' Aadhaar Enabled Bank Account (AEBA)
- Aadhaar Enabled Payment System (AEPS) – A system that leverages Aadhaar online authentication and enables AEBAAs to be operated in anytime-anywhere banking mode by the marginalized and financially excluded segments of society through micro-ATMs

Aadhaar Payments Bridge is a repository of Aadhaar number of residents and their primary bank account number used for receiving all social security and entitlement payments from various government agencies. APB requires using Aadhaar number as the primary key for all entitlement payments. This would weed out all fakes and ghosts from the system and ensure that the benefits reach the intended beneficiaries.

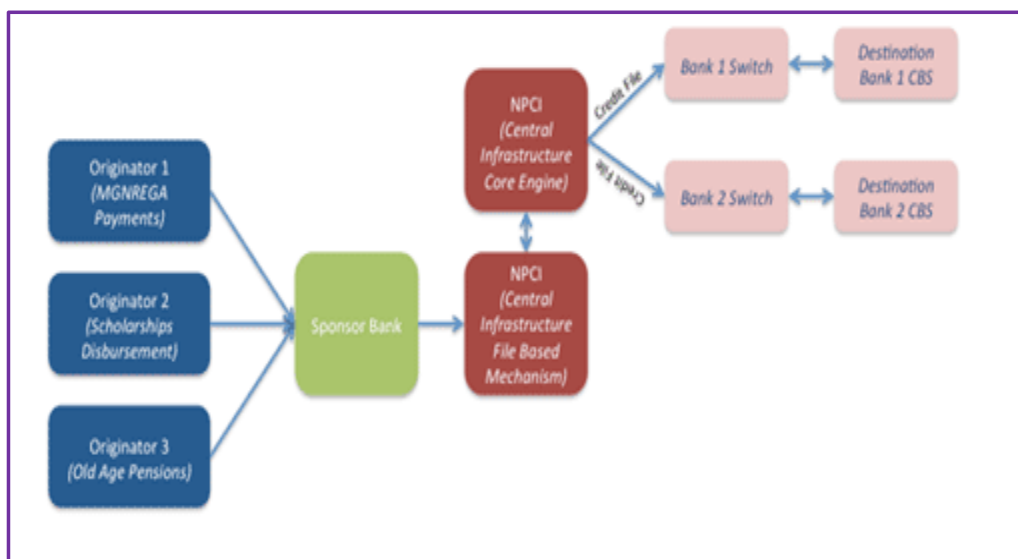


Figure 5: Aadhaar Enable Payment

The key steps in posting payments via APB are:

- Service delivery agency that needs to make payments to its beneficiaries (such as MGNREGA wages, scholarships disbursement, old age pension etc.) provides APB file containing details of Aadhaar number, welfare scheme reference number and the amount to be paid to its bank.
- The sponsor bank adds bank IIN (Institute Identification Number provided by NPCI to participant banks) to the APB file and uploads onto NPCI server.
- NPCI processes uploaded files, prepares beneficiary bank files and generates settlement file
- Settlement file is posted to bank accounts with RBI

Aadhaar Enabled Payment System empowers the marginalized and excluded segments to conduct financial transactions through micro-ATMs deployed by Banks in their villages.

The key steps in doing transactions via AEPS are:

- Resident provides his/her Aadhaarnumber, details of financial transaction sought and fingerprint impression at the micro-ATM device.
- Digitally signed and encrypted data packets are transferred via Bank Switch to NPCI to UIDAI.
- UIDAI processes the authentication request and communicates the outcome in form of Yes/No.
- If the authentication response is yes, bank carries out the required authorization process and advises micro-ATM on suitable next steps.

5.5. Updation

The Aadhaar holders will have an option to update their demographic and personal details stored in the CIDR. This is in order to facilitate the correction of any mismatch of their details and also updating certain details like current address etc.

The process would involve an initial authentication with Aadhaar number and biometric details. After successfully authenticating, the holder can update his/her records accordingly. The exact process and details of the ecosystem partners involvement will be updated shortly on the UIDAI website.

5.6. Reporting (BI and Portal)

- i. All the statistical information collected by the UIDAI, including aggregated demographic data, process data, and usage information is made available to the public through the UIDAI web portal. If information could be available to citizens through the RTI act, the information must be available to all on the portal.
- ii. However, individual resident's information is not made available through this interface.

6. UIDAI Infrastructure

6.1. Physical Infrastructure

UIDAI's physical infrastructure is critical for facilitating seamless delivery of key objectives of the UID project. Thus, while designing security measures for UIDAI, consideration of physical infrastructure is highly recommended. Primarily, following components are involved:

- i. **Primary Data Center:** This facility would host the datacenter from where UIDAI's services would be delivered during normal course of affairs. It would have appropriate physical and environmental security controls built-in to provide physical security to IT infrastructure, storage media, people and overall building infrastructure.
- ii. **DR center:** Disaster recovery center is to be put in use essentially to maintain continuity of UIDAI's services during a pre-defined disaster scenario at the primary datacenter. Data repository at this facility would be replicated/synced with primary datacenter using adequate & secure network connectivity options. This facility

- should have similar physical and environmental security controls as applicable to the primary datacenter.
- iii. **Other Facilities:** Facilities of ecosystem partners/agencies associated with UIDAI operations would fall into this category. Since these locations are important within the context of storage, processing and transmission of PII information and/or UIDAI's operational information, these premises are key physical components in the overall setup of UIDAI and thus need to be adequately protected in line with UIDAI's policies and secure implementation principles.

7. Understanding the UID Technology Solution

India will be the first country to implement a biometric-based unique ID system on such a large scale. UID will serve as a proof of identity, allowing residents to establish their credentials anywhere in the country.

The UID based approach creates an authentication system and gives the UIDAI ability to confirm an individual's identity. The diagram below provides a high level view of the overall UID Technology Solution.

7.1. UID-Technology Solution Architecture Development

- i. UID-TS architecture has been developed with increasing level of details, all the way from intent to implementation. Figure 6 below shows the 'onion peeling' method of this development. At the core is the UIDAI intent that drives the creation of system architecture which in turn drives the development of application and data architectures. The applications have to be translated to implementation architectures using the cloud and grid with right technology stacks. Scaling and Transitioning are also addressed as part this massive exercise of giving AADHAAR to 1.2 billion people. Finally the architecture acts as one of the inputs to creation of suitable business models and the services framework.
- ii. Rest of this introductory section follows the same as the architecture development. The business model and services are left out.

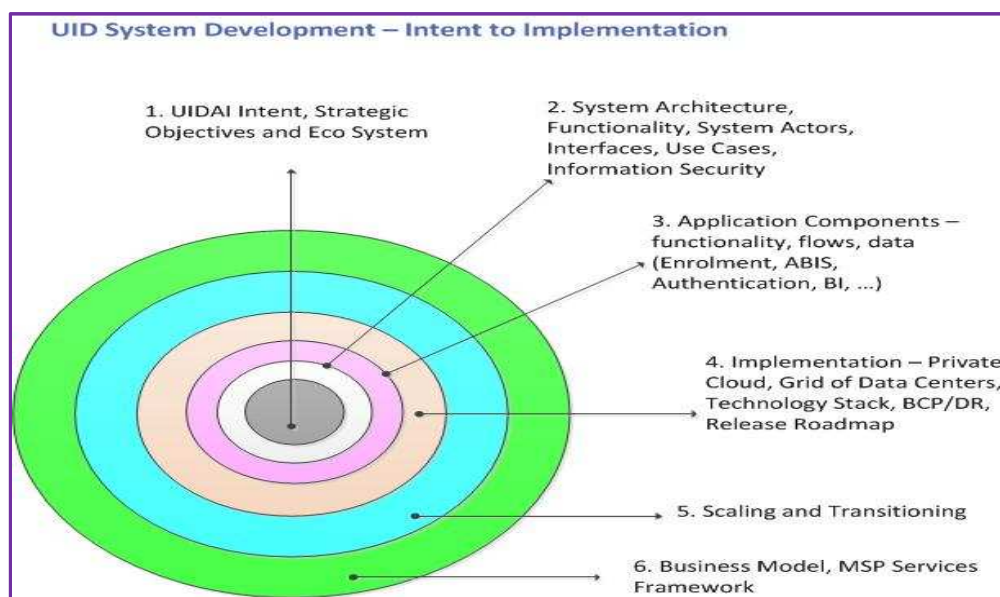


Figure 6: UID System Development – Intent to Implementation

7.2. UID System Functional Overview

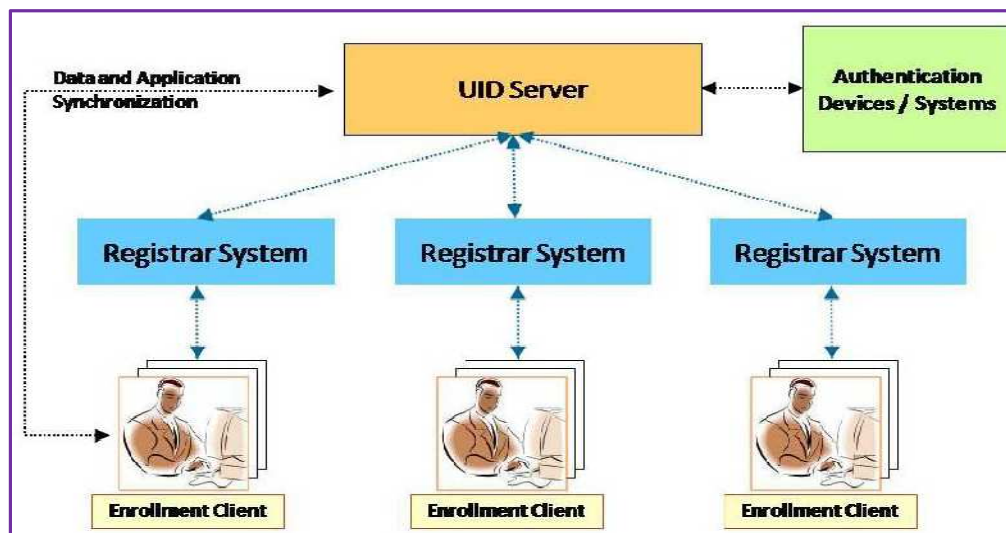


Figure 7 : High Level System Overview

7.3. Structure of UID Technology Solution

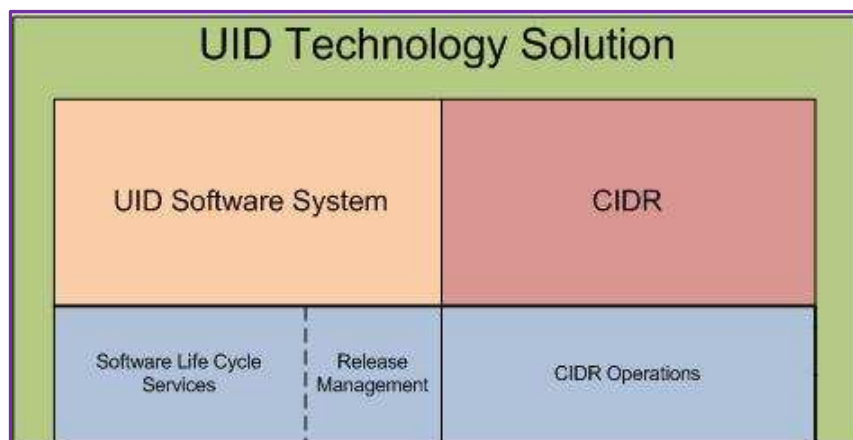


Figure 8 : Overview of UID Technology Solution

- i. The UID Technology Solution encompasses all application software, system software, infrastructure (including IT systems, Private Cloud of Data Centres). It also encompasses all the processes required to architect, design, develop, release, deploy and manage the solution and manage the cloud & data center operations.
- ii. The UID Software system consists of the enrolment client application, enrolment and authentication server applications, AADHAAR Unified portal, Business Intelligence Module, Fraud Detection Module and the entire supporting software platform.
- iii. The CIDR refers to the infrastructure including NOC, Cloud of Data Centres, Network, Servers and Storage, for production, staging and testing.
- iv. The Software lifecycle services refer to the entire lifecycle processes required to collect requirements, prototype, architect, design, develop, test and release various software components as part of the overall UID Software system
- v. The Release management process ties the UID Software system and the CIDR through rigorous release and rollout of the software into various environments such as staging and production
- vi. The CIDR operations refer to the managed services required to operate the cloud of data centers and associated infrastructure (Network, Servers, Storage, Power, and HVAC).

The diagram illustrates the Aadhaar Partner Eco-systems architecture, showing the central role of the UID App Server and its interactions with various stakeholders and services.

Central Core:

- UID App Server:** The central hub, containing:
 - Biometric Middleware:** Admin, BI, Portals, Enrollment, Authentication.
 - Biometric System:** V1, V2, V3.
 - CIDR (Logically Centralized):** Biometric Service Providers (BSPs).

External Services and Partners:

- Letter Delivery:** India Post.
- Aadhaar Letter Printing:** Manipal Tech, Sesha Sai, KL Hitech.
- Contact Centre System:** IntelliNet.
- Banks** and **KYC Agencies**.
- Operator Testing & Certification Agency:** SIFY.
- Enrolling Agency:** 300 Enrolling Agencies.
- Registrar:** State Govts, Banks, LIC etc.
- Device Testing & Certification:** STQC.
- ASA (Authentication Service Agency):** Telecoms etc.
- AUA (Authentication User Agency):** State Govts, Banks etc.
- Mobile Gateway Providers:** Telecoms etc.

Enrolment and Authentication:

- Enrolment Client:** Interacts with **Enrolment Devices** and **Authentication Devices**.

Figure 9 : UID System Overview

Referring to

, we have 3 main parts namely

- i. UID Technology Solution(UID-TS) comprising
 - a) UID Software System
 - b) CIDR
- ii. Partner Systems interacting with the UID-TS for such as
 - a) Registrar System
 - b) Contact Center System
 - c) Logistics System

- d) Authentication User Agencies
- iii. UID Stakeholder Ecosystem comprising
 - a) Registrar Management
 - b) Enrolment Agency Empanelment
 - c) Training Agency Empanelment
 - d) Device Certification
 - e) Testing and Certification Agency

The software system has the following components

- i. Core UID Application consisting of
 - a. Enrolment Application
 - b. Authentication Application
- ii. Biometric System for de-duplication
- iii. Supporting Applications such as
 - a. Administration
 - b. Analytics and Reporting or Business Intelligence
 - c. Fraud Management
 - d. Portals for Partners and Public
 - e. Customer Relationship Management (CRM) for Contact Center Interface
 - f. Logistics Interface Application
- iv. Other Applications such as
 - a. Hosted Client /User/3rd party applications (e.g. PDS, NREGA, ...)
 - b. Document Management

In the following sections of this Introduction we shall explain each of the above components.

7.4.2. UID Application

7.4.2.1. Overview of UID applications

- i. The application hosted by CIDR can be broadly categorized under the core applications and supporting applications are described in Figure 10 **Error! Reference source not found.** In the core category we have the enrolment and authentication applications services. While the supporting category consists of applications required for administration, analytics, reporting, fraud detection interfaces to Logistics Provider and Contact Center and the portal.
- ii. The *Enrolment Application* services the client enrolment request for providing a UID. The enrolment application orchestrates the enrolment workflow by integrating various sub-systems such as demographic data validation, biometric de-duplication, and UID generation. Need to talk about lifecycle updates (not only initial enrolment)

- such as correction, on-going updates, child re-enrolments, death reporting, etc. Manual Exception Workflow is required to resolve Enrolment requests that cannot be resolved automatically. Basic Letter Printing and Delivery functionality is available for servicing exceptions to normal workflow.
- iii. The ***Authentication Application*** provides the identity authentication services. Various authentication request types such as demographic, biometric, simple or advanced authentications are supported. The UID number submitted is used for 1:1 match for the resident's record. The inputs are then matched against the resident information stored in CIDR databases to authenticate the resident.
 - iv. The ***Fraud Detection Application*** is deployed to detect and reduce identity fraud. For example identify fraud scenarios that the application needs to handle are: misrepresentation of information, multiple registrations by same resident, registration for non-existent residents, or authentication as someone else. Multiple approaches are used for detecting fraud. In **Rule based** fraud detection, the fraud engine will detect fraud based on pre-defined set of rules. The engine will process the enrolments/authentications based on these rules and automate the decision to accept, reject or forward for manual inspections. In fraud **prediction model**, the fraud engine uses "prediction algorithms" to assign risk scores for the transactions. The ones that have reached a threshold are categorized as fraud or investigated further. **Manual inspection** involves review of potential fraudulent transactions by analysts. By using this in conjunction with rule based and prediction model, only a subset of transactions will be submitted for manual inspection.
 - v. The ***Administrative Application*** takes care of user management, roles and access control, business process automation, and status reporting. It ensures a trust network across both internal and external entities. The external entities could be registrars, enrolment agencies, field agencies, introducers, Authentication User Agencies, and other partners within the eco system. For example the application is required to manage user accounts for the registrar users or introducers who vouch for identity of individuals who lack proper documentations. The internal entities could be system administrators, customer service agents, biometric and fraud detection agents. The application will allow administrators to track status of use cases, and provide mechanism to escalate failures or delays.

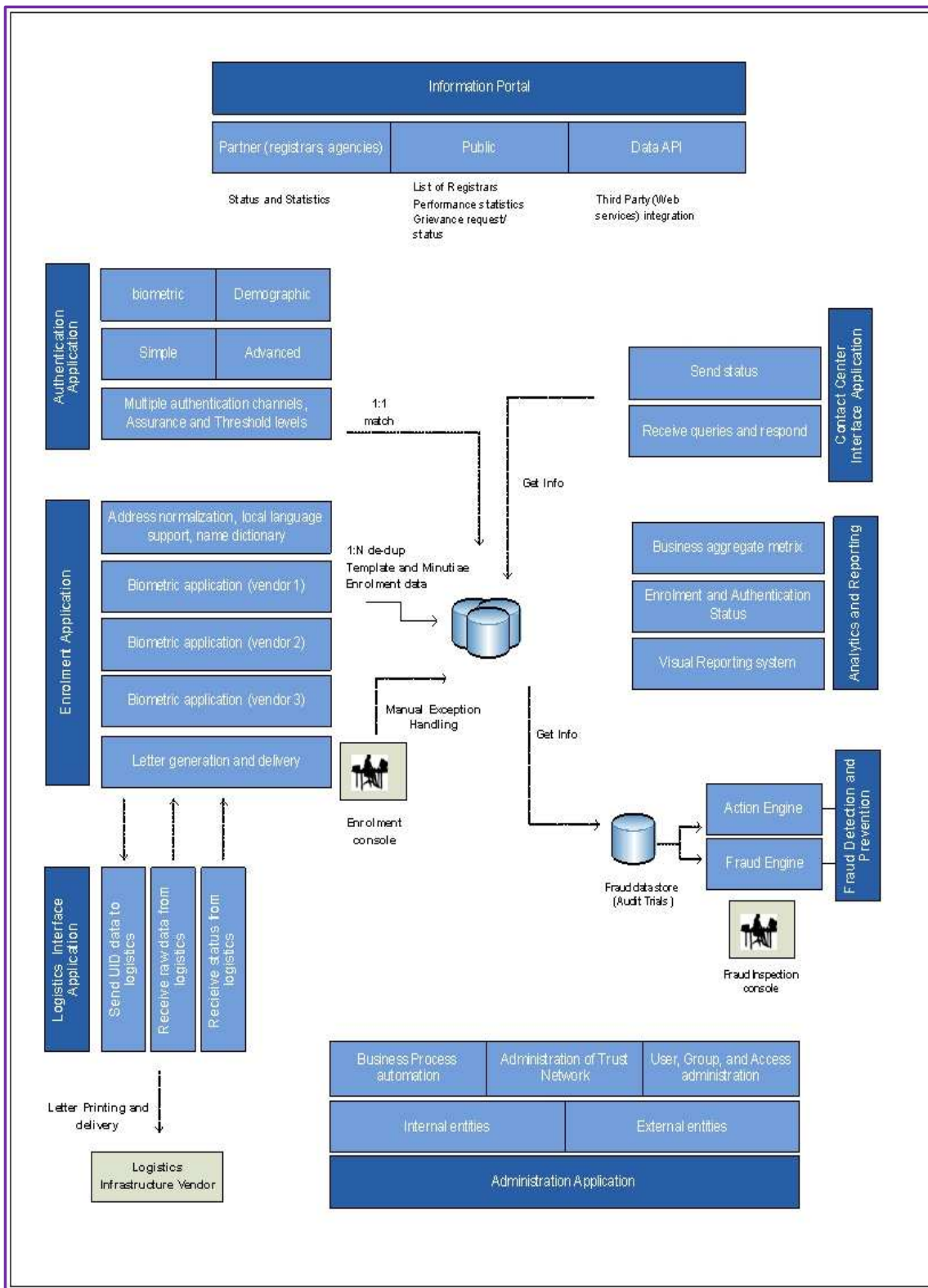


Figure 10: UID Application hosted in CIDR

Other application interfacing with UID Applications

- i. The **Analytics and Reporting Application** provides enrolment and authentication statistics for both public and partners. It supports visual representation of statistics and allowing drill down at region levels. All the information available for this application is only at the aggregate level and does not contain any personal identifiable information thus ensuring individual identity is completely protected.
- ii. **The Information Portal** provides an administrative and information access for internal users, partners and for public. Besides the above Application, interface application for Logistics and Contact Center are also present in the CIDR.
- iii. **The Contact Center Interface Application** provides inbound and outbound channels to manage all queries, status enquiries and grievances from residents, registrars and enrolment agencies and other stakeholders of UID ecosystem.
- iv. **The Logistics Interface Application** interfaces to the Logistics Provider for letter printing and delivery. It is used for sending and receiving raw data, sending UID data for letter printing and delivery and receiving daily status updates on the inbound and outbound sides. The Logistics Application tracks the delivery of enrolment packets from enrolment agencies to CIDR and delivery of printed UID letter to the Resident.

7.4.3. Biometric Solution

- i. Three biometric Solution Providers have been selected by UIDAI to operate simultaneously in CIDR as a UIDAI strategy. This strategy has evolved as biometric solution for our large population is a challenge.
- ii. Two biometric components are utilized in the UID System. The biometric components are:
 - a) **Automated Biometric Identification Subsystem (ABIS):** ABIS will be used in the Enrolment Server as a part of the multi-modal biometric de-duplication solution. In the early release, ABIS will also be used in the Authentication Server for verification. The ABIS will maintain its own database of proprietary fingerprint and iris templates for de-duplication (and face templates at the discretion of the vendor), and must be able to respond to verification requests accompanied by fingerprint and/or iris images, as well as ISO/IEC 19794-2:2005 format fingerprint minutiae files. Vendors will work with the UIDAI to provide further specification within 19794-2 to promote interoperability with future verification clients.
 - b) **Multimodal SDKs:** SDKs will be used in the enrolment client, manual check (for duplicates), authentication server (for later releases) and the analytics

- module. The SDK may contain signal detection, quality analysis, image selection, image fusion, segmentation, image pre-processing, feature extraction and comparison score generation for fingerprint, iris and face modalities.
- iii. The biometric solution components used in the UID system are:
 - a. Multi-modal de-duplication in the enrolment server
 - b. Verification subsystem within the authentication server
 - c. Enrolment client
 - d. Manual checks and exception handling
 - e. Biometric sub-system monitoring and analysis
 - iv. The functional requirements of the five areas are described, followed by the overall functions of the two biometric components.

7.4.3.1. UID System Requirements of the biometric components

7.4.3.1.1. Multi-modal Biometric de-duplication in the Enrolment Server

- i. Considering the expected size of the de-duplication task, the UID enrolment server will utilize:
 - a) **Multi-modal De-duplication:** Multiple modalities – fingerprint and iris will be used for de-duplication. Face photograph is provided if the vendor desires to use it for de-duplication. *While certain demographical information is also provided, UIDAI provides no assurance of its accuracy.* Demographic information shall not be used for filtering during the de-duplication process, but this capability shall be preserved for potential implementation in later phases of the UID program. Each multi-modal de-duplication request will contain an indexing number (Reference ID)¹ in addition to the multi-modal biometric and demographic data. In the event one or more duplicate enrolments are found, the ABIS will pass back the Reference ID of the duplicates and the scaled comparison scores upon which the duplicate finding was based. The scaled fusion score returned with each duplicate found will have a range of [0, 100], with 0 indicating the least level of similarity and 100 as the highest level of similarity.
 - b) **Multi-vendor:** Multiple complete multi-modal solutions from more than one vendor will be used as shown in The UID Application will determine routing of a particular de-duplication request. It may decide to route a particular de-duplication request to more than one biometric solution. If it routes a de-duplication request to more than one solution, it is responsible for determining the final outcome of the de-duplication request. The UID ABIS API specifies the interaction between UID Application and ABIS.

¹ ABIS will not be aware of the UID #, nor will it be aware of how UID #maps to reference ID or records in the reference DB.

- c) **The UID Biometric middleware** included in the UID application (being developed by ASDMSA) is meant to provide vendor independence and standardization. The key features of the middleware is
- Routing and mediation.
 - Guaranteed delivery
 - Fault tolerance and load balancing
 - Open standard based messaging (Advanced Message Queuing Protocol) using open source RabbitMQ
 - Transparent connectivity to analysis and system monitoring modules of UID applications
 - Support of web 2.0 based UID ABIS API and CBEFF data format standard
 - Encapsulation and isolation of ABIS components

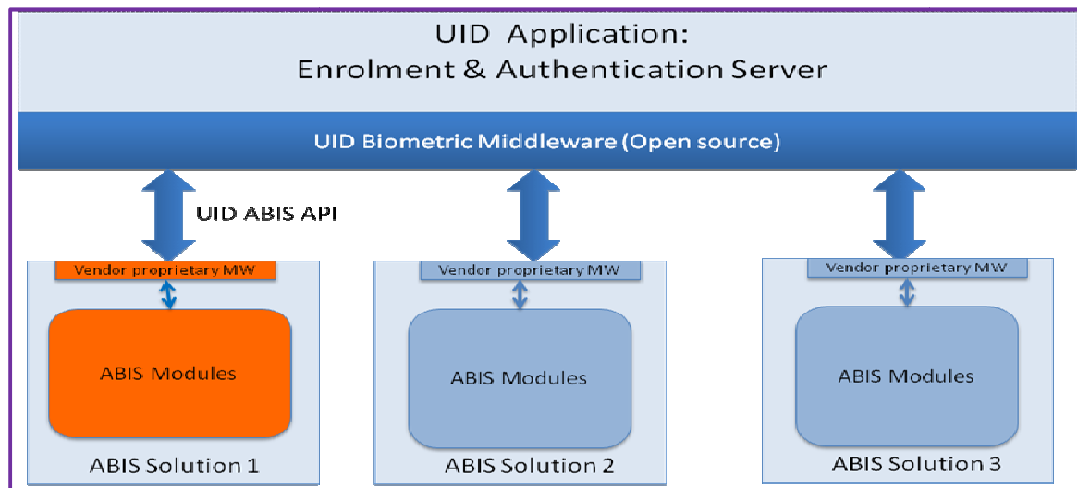


Figure 11: UID Application and ABIS Integration

7.4.3.2. Verification or Authentication Server

The Authentication Server works outside the ABIS solution components which are used for de-duplication during enrolment. The solution is capable of 1:1 verification comparisons of enrolled references with incoming ISO/IEC 19794-compliant fingerprint, iris or face images or 19794-2 compliant fingerprint minutiae sets without proprietary extended data.

- Illustrates both the verification and de-duplication subsystems to be supplied by the BSP.
- For the purpose of distributed authentication by UIDAI at a later stage, the biometric verification module may be constructed using SDK. While the functionality of the verification subsystem will not change, the internal architecture may change. The templates will be maintained in memory resident database by the UID authentication server application (not in scope of BSP). If the incoming

requests contain a biometric image, the Authentication server will use SDK to extract the feature. SDK will also be used to generate comparison score of the sample. UIDAI has decided to go with a distributed authentication application to achieve required service levels.

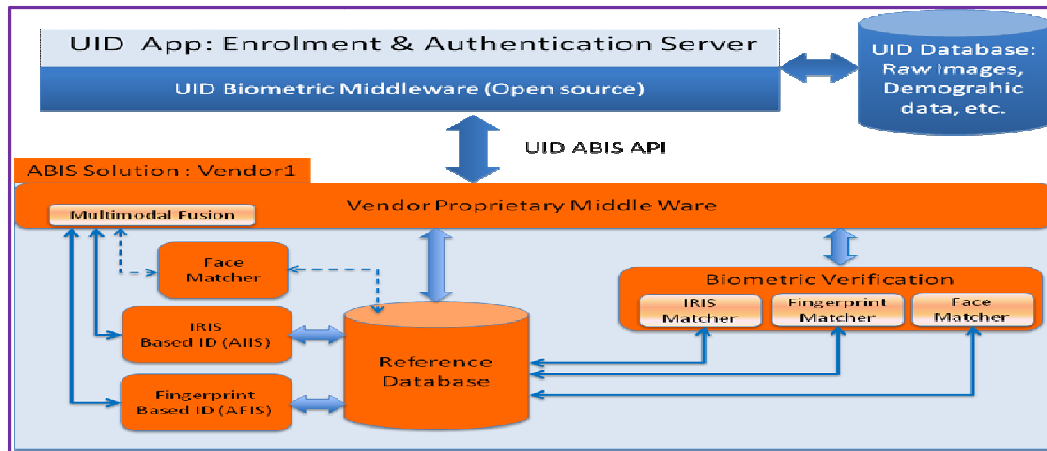


Figure 12: ABIS Solution

7.4.4. UID Business Intelligence (Analytics and Reporting)

7.4.4.1. Introduction

- i. The execution of various business processes in the UID application like enrolment, authentication and update is likely to generate large amounts of event related data which can be transformed into useful information/ progress indicators for the purposes of public viewing, partner monitoring and in some special situations also aid in research.
- ii. The Analytics and Reporting module will publish these aggregate numbers for end user consumption, including general public. A visual reporting system comprising of GIS, graphs and pie-charts with drill down capabilities is envisioned in order to make the information user-friendly and accessible.
- iii. Besides the Analytics and Reporting module will also provide reports on the business process of Enrolment and Authentication as well as the subsystems and users involved in the handling of these sub-systems. Aggregate statistics, by region, are presented visually with the help of a map where appropriate, which allows users to drill down on regions, and get statistics.
- iv. The UID Business Intelligence (UIDBI) Application intends to serve the following segments of the users
 - a. Managed Service Provider

- b. Partners and Registrars
- c. General Public
- d. External Application developers
- e. Statisticians and Analysts
- f. Users within UIDAI

7.4.4.2. UID-BI Functions

The Proposed implementation architecture for UIDBI shall consist of the following components.

- i. UIDBI Atomic Data Warehouse consisting of atomic data obtained synchronously or asynchronously from the UID-Server, time-variant, consolidated, aggregated minimally to provide such information for downstream needs, such as data marts, Charting applications, sandbox etc.
- ii. UIDBI Data marts consisting of subject area specific or other subsets specific data derived from the UIDBI data warehouse through a process of aggregation, along with relevant dimensionality
- iii. UIDBI EAI consisting of tools and applications to provide for extraction of data from source systems into the UIDBI Data Warehouse
- iv. UIDBI Analytical and reporting delivery platform consisting of tools and platform to deliver all relevant metrics, dashboards, portals, reports, action-response work-flows etc.
- v. UIDBI Metadata layer consisting of tools to define, maintain and browse the definitional layer of the UIDBI through its complete lifecycle. This needs to be revisited based on the toolsets capability to provide for such capability.
- vi. UIDBI security and administration layer, integrated with the UID main security and administration layer inclusive of ACLs
- vii. UIDBI Sandbox to provide secure downloads from the UIDBI Database for purposes of advanced analytics and modeling
- viii. UIDBI Data distribution platform used to provide data in various forms for use by internal and external applications.

7.4.4.3. Overview of the Proposed Solution Architecture for UID-BI

UID requires a highly scalable, n-tier, reliable and open technology components to meet the UIDBI requirements. The solution architecture is shown in

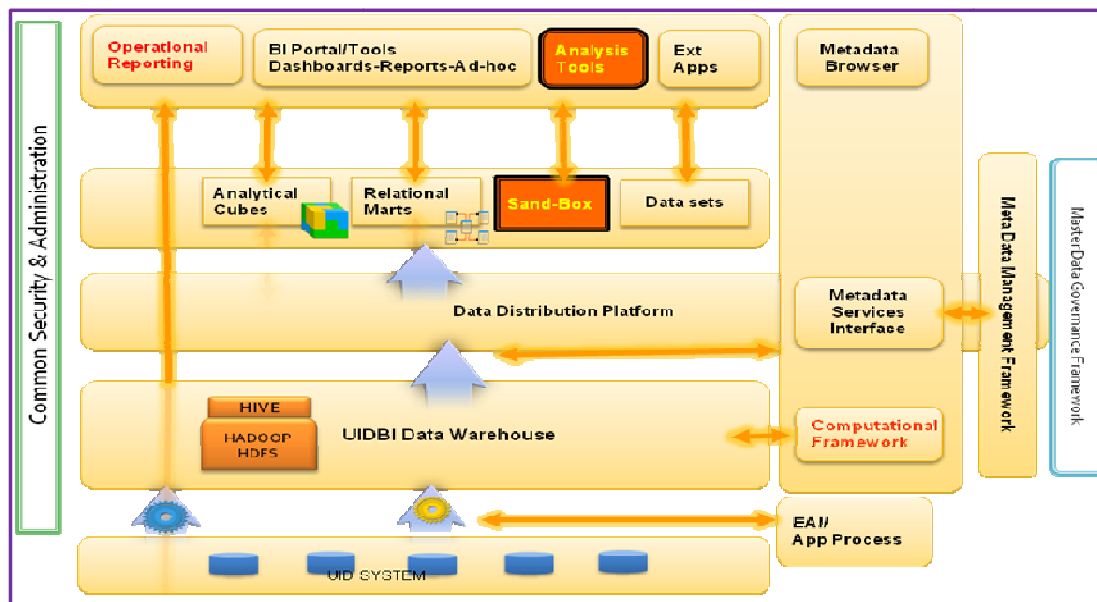


Figure 13: UID Analytics and Reporting Subsystem

7.4.4.4. Analytics and Reporting

- The UID - Analytics and Reporting subsystem (UIDBI) provides an extended set of metrics to monitor the progress, usage and status of the UID ecosystem. The output is proposed to be delivered as a distinct set of metrics through various portals viz. Partner portal, Public information portal, Data portal etc.

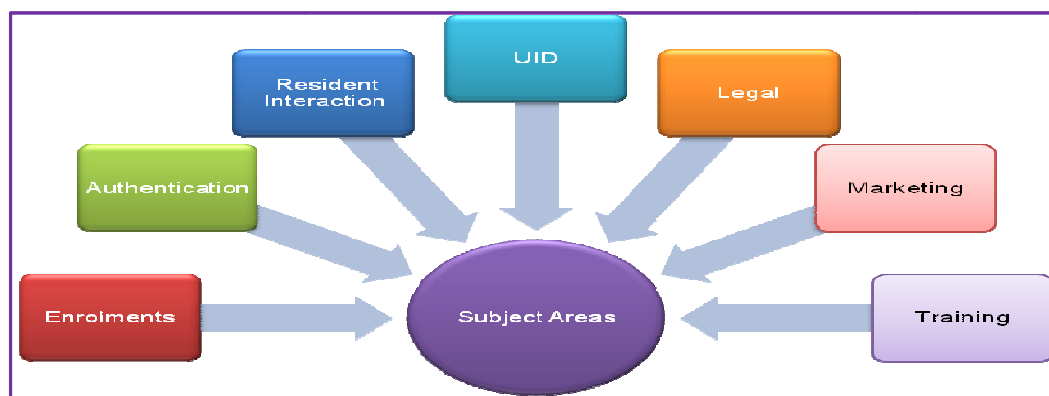


Figure 14: UIDBI Subject Areas

7.4.4.5. Information Portal

- i. The information portal will provide an overall dashboard to track the performance of the UID system, in addition to providing a variety of standard reports. This is divided into the following portals.

7.4.4.6. Partner Portal

- i. The UID project is based on a partnership model consisting of Registrars and their respective enrolling agencies on the ground. There are other entities such as device suppliers, trainers, letter delivery agencies, pre-enrollers etc. all of whom play an important role in enrolling 1.2 billion residents. The partner portal will cater to the needs of the partner community.
- ii. This portal will provide them with overall statistics for use cases that involve them, as well as allow them to track individual cases.
- iii. These users will be able to track:
 - a. Administration, and User management – creation / deletion of the user records
 - b. Aggregate Pre-Enrolment stats for them – number, latency, validation issues. (for Registrars, Sub-Registrars, and Enrolment Agencies)
 - c. Aggregate Enrolment statistics for them – number, latency, approvals, rejection reasons (for Registrars, Sub-Registrars, and Enrolment Agencies)
 - d. Aggregate Authentication statistics for them – number, latency, success / failures (for authentication clients)
 - e. Track individual resident cases – pre-enrolment, enrolment, and authentication – that they are involved in.

7.4.4.7. Public Portal

- i. The UID being a project of national importance will need to continually share various design, development, implementation and operational aspects with the public. The grievance redressal system needs to also be integrated into the public portal in order to redress complaints and grievances faced by residents in the process of enrolment or authentication. The UID information portal will address the above needs. This portal will also provide all users with information about the UID system, and allow them to drill down on the performance by region, etc. It will not allow users to track individual cases.
- ii. However, a method will be provided to get in touch with the UID for specific questions, as well as addressing grievances.
- iii. All users will be able to see:
 - a. List of Registrars, Enrolment Agencies, etc.

- b. Number of UIDs issued by time (day, month, year), and region (country, state, district, city)
- c. Performance Metrics – At an aggregate level – the number of Registrars, latency to allocate UIDs, number of complaints, etc.
- d. Authentication requests – count, latency, success / failures.
- e. Grievance requests filed with the UIDAI, and the responses.

7.4.4.8. Data Portal

- i. We want to expose all publishable public information through a “Data Portal” where all data is exposed in machine readable formats. This portal allows 3rd party developers to develop web 2.0 applications based on this data.

7.4.5. External Interfaces

7.4.5.1. Registrar System

- i. Registrars will have their own IT infrastructure to interact with Aadhaar System. The functionalities include:
 - a. Getting updates during enrolment process
 - b. Uploading bulk demographic data
 - c. Act as an Authentication User Agency (AUA)
- ii. A copy of the enrolment data flows from the Enrolment Stations to the Registrar System. The CIDR also updates the Registrar System with the assigned UIDs.
- iii. In order to keep the confidentiality of the data being sent to the registrar system, the data will be encrypted using the public key provided by the registrar. It follows that the Registrars have to manage their <Private Key, Public Key> pair securely and put the necessary infrastructure in place. The interacting Registrar systems have to be hardened. UIDAI may provide security guidelines to Registrars to assist in the implementation but the ownership will always reside with the Registrars.
- iv. UIDAI will define interfaces for the Registrar System to interact with CIDR. There will be no libraries to be integrated with.
- v. Since the Registrars also maintain a copy of their enrolments data, they have to take enough precautions to secure the data.
- vi. In order to integrate Aadhaar authentication with applications like PDS, NREGA or similar applications in private sector, UIDAI will provide a library of API using which the new applications can be developed and deployed.

7.4.5.2. Logistics

- i. Logistics service is currently provided by Department of Posts. Figure below shows the broad functions currently performed by Department of Posts.

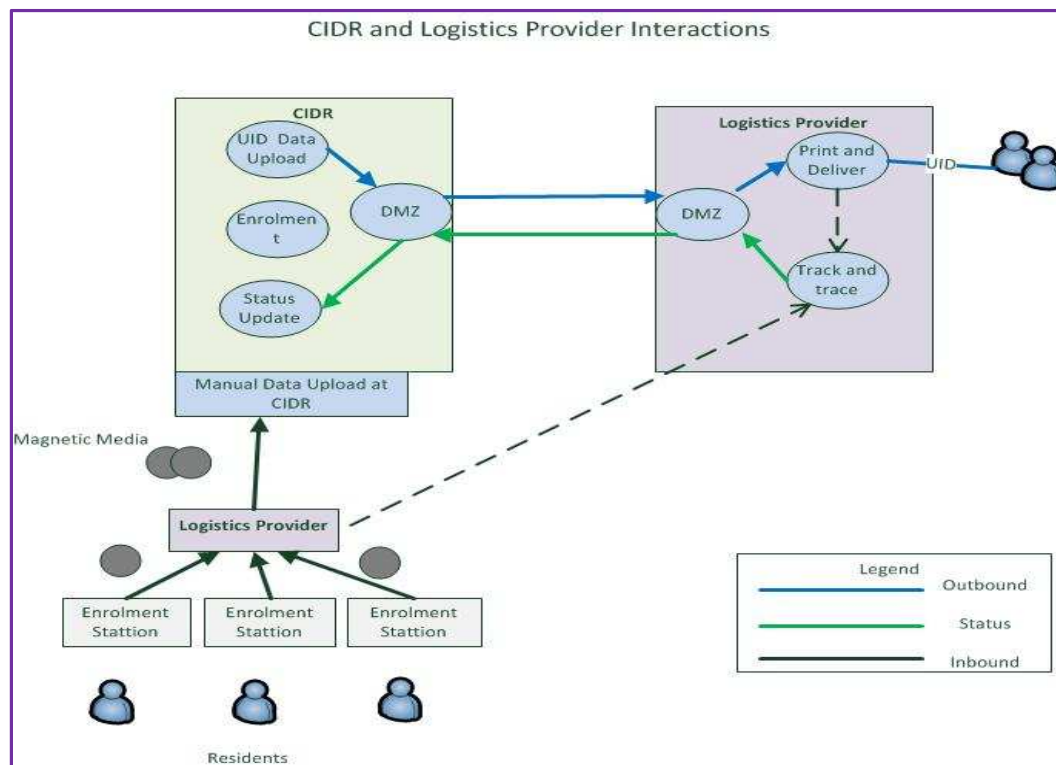


Figure 15: CIDR and Logistics Provider Interactions

- ii. Responsibilities of Logistic Service Provider includes,
 - a. Logistics setup for enrolment agencies to send the enrolment data/manifest to the RO/data centre.
 - b. Provide printing infrastructure and connectivity to the CIDR. The printing infrastructure electronically receives the UID allocation letter to be printed and mailed to the enrolled residents.
 - c. Mail the printed UID letter to the enrolled resident.
 - d. Provide an online track and trace system to track the status of the enrolments and UID generation.
 - e. Provide updated status of enrollments through the ASK, UID Portal, SMS etc. as the case maybe

7.4.5.3. Authentication User Agency

Authentication User Agencies (AUA) are responsible for handling and processing authentication requests from service providers and interacting with Authentication Service agencies. Before providing a service to a resident the service provider needs to verify authenticate the identity of the resident. It forwards the authentication request to an AUA which contacts with the ASA which in turn send the request to the CIDR which finally verifies the identity.

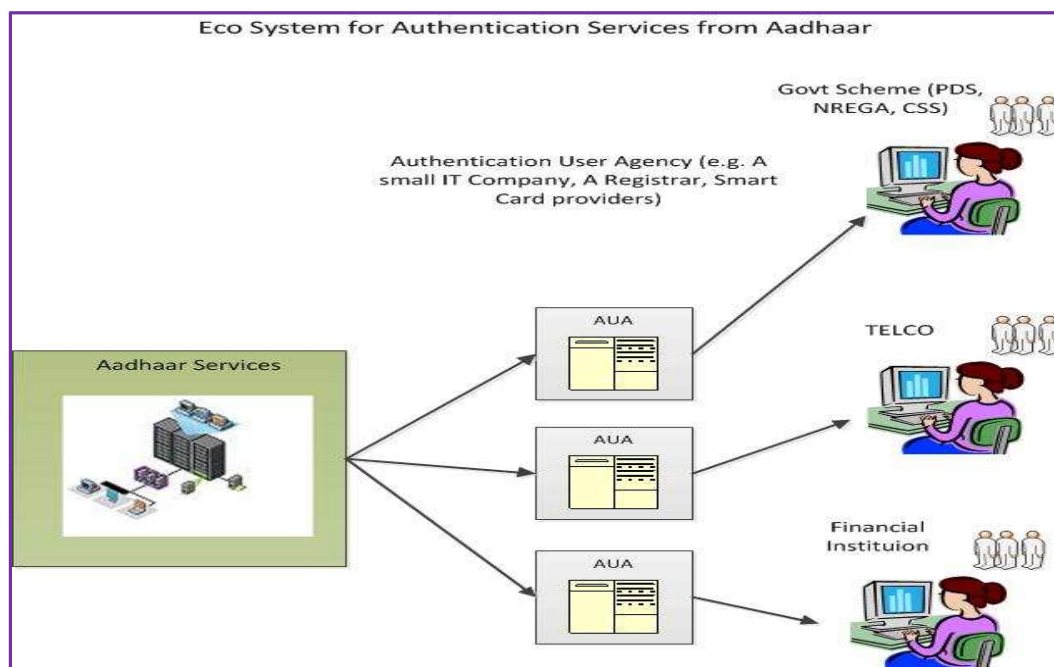


Figure 16: AADHAAR Authentication eco system

The applying bodies have to follow a mandated procedure to become AUAs (detailed procedure given on the UIDAI website). It would need to engage with the respective ASA relevant to its business purpose and establish a connection with the ASA.

7.4.5.4. Authentication Service Agency

ASAs are entities that have secure leased line connectivity with the CIDR. ASAs transmit authentication requests to CIDR on behalf of one or more AUA. They will accumulate all the requests from the various AUAs connected to it and send the requests to the CIDR to facilitate the authentication transactions.

The applying bodies have to follow a mandated procedure to become AUAs (detailed procedure given in the UIDAI website).

7.4.5.5. Contact Center

- i. The Contact Center provides a central point of contact to residents and other entities that will partner with UIDAI during the enrolment and post enrolment stages. The Contact Center will provide services in multiple languages for residents, registrars, enrolment agencies and resident service agencies.
- ii. The Service Provider for Contact Center will setup, operate and maintain the Contact Center including the agents. The Service provider for Contact Center will be expected to,
 - a. Scale operations at the required pace to match volumes of interactions
 - b. Provide analytics support to UIDAI
 - c. Assist in driving performance improvements
 - d. Take end to end responsibility of driving resolution of queries and services
 - e. Analyze the various interactions with the stakeholders, identify and develop process models
- iii. The RFP for Contact Center contains the detailed requirements for Contact Center. Please refer to this document from UIDAI website.
- iv. The Contact Center Architecture diagram is shown in below.

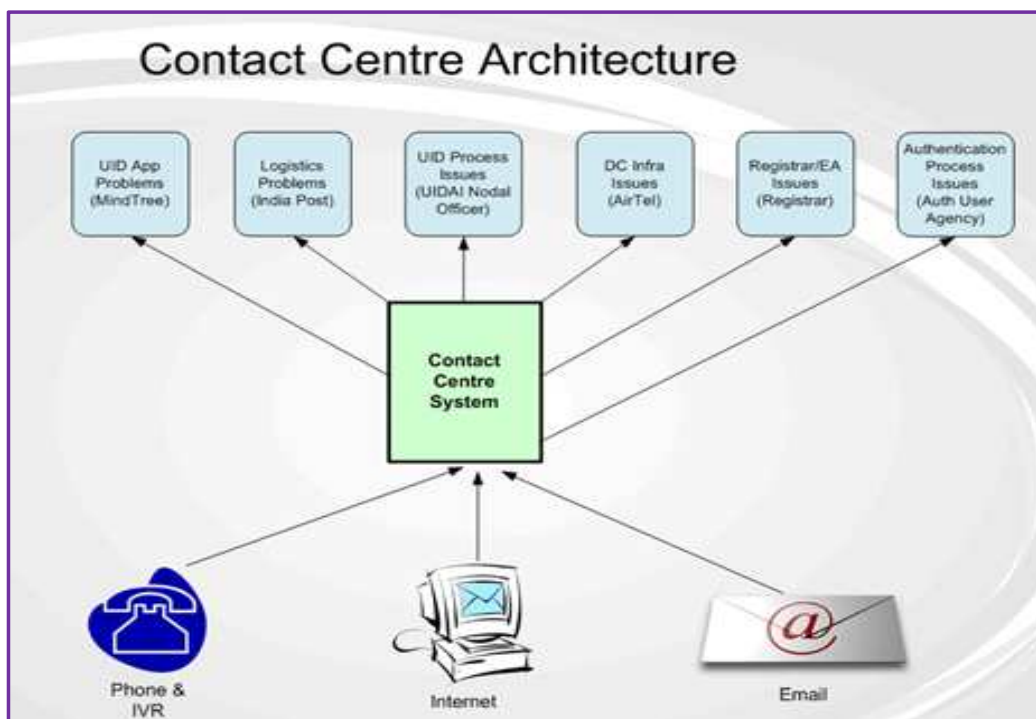


Figure 17: Contact Centre Architecture

7.5. Information Security

- i. Protecting the CIDR and the supporting resources is of prime importance since the misuse of the system can render the UIDAI program ineffective. Apart from protecting the UID number adequate security should also be extended for the technology and the processes surrounding them to provide a holistic view of security of the UID system.
- ii. The following diagram highlights the touch points of the UIDAI system with residents. At each of these points, the UID has the possibility of gathering data, and providing services to the residents. These touch points are also important from a security perspective, as these represent the points at which external security threats could emanate, and each of these becomes a threat zone.

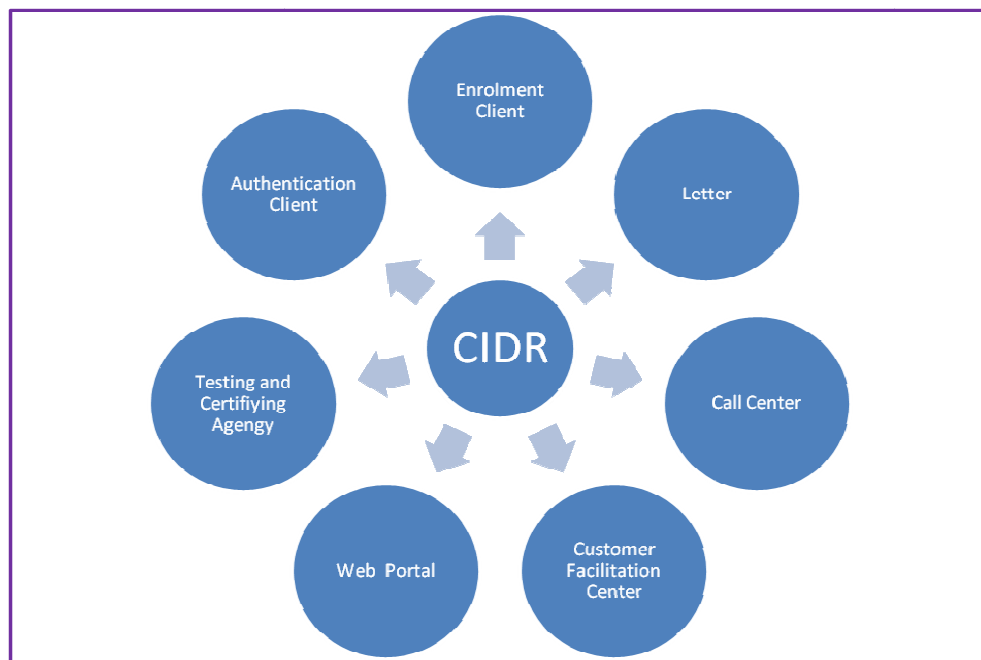


Figure 18: UIDAI System touch points

7.5.1. Information Privacy and Data Security

- i. The UIDAI is collecting, what is generally described as Personal Identifiable Information (PII). As a consequence, it is advisable to clearly and publicly state how this data will be used, and how will it be protected from unauthorized access. Even though the UIDAI stores resident information and confirms identity to

- authenticating agencies, it will have to ensure the security and privacy of such information.
- ii. By linking an individual's Personal Identifiable Information to a UID, the UIDAI will be creating a transaction identity for each resident that is both verifiable and reliable. This means that the resident's identity will possess value, which shall enable service delivery.
 - iii. The UIDAI envisions storing basic personal information, as well as certain biometrics. However, limiting its scope to this, and not linking this information to financial/other details does not make the resident records in the database non-sensitive. Biometric information for example, is often linked to banking, social security and passport records. Basic personal information such as date of birth is used to verify owners of credit card/bank accounts and online accounts. Such information will therefore, have to be protected. Loss of this information risks the resident's financial and other assets, as well as reputation, when the resident is a victim of identity theft. In the federated system that the UIDAI envisions, it must be ensured that there are processes in place to make sure a strong level of data security.
 - iv. The following security framework summarizes the set of measures required to protect the PII from theft.

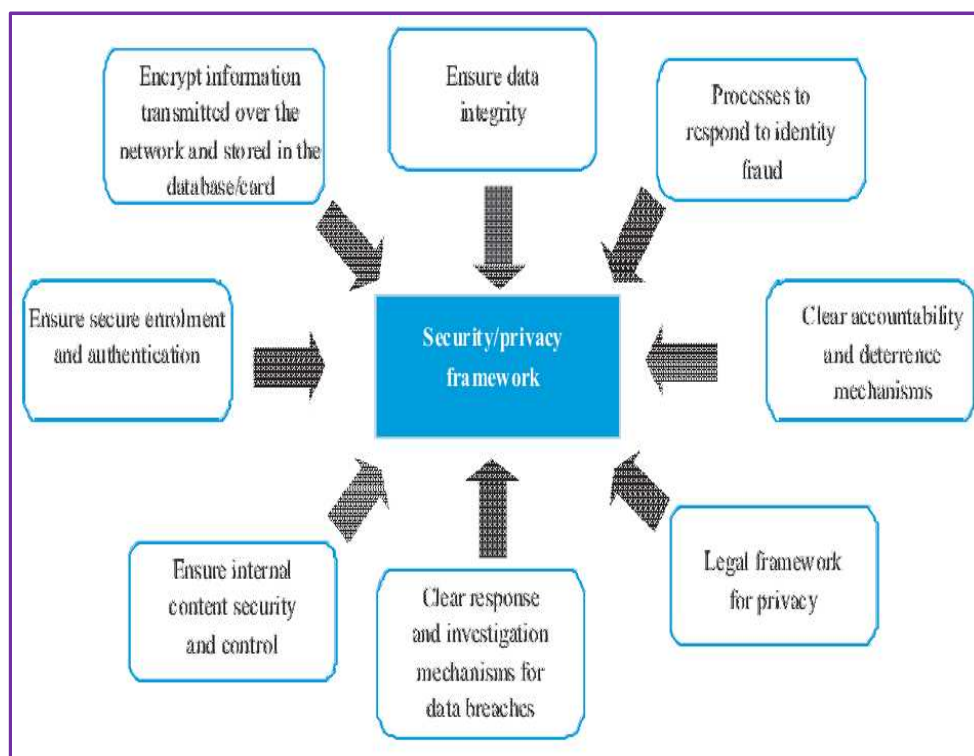


Figure 19: Security Framework

7.5.2. IT Infrastructure Security Requirements

Information technology infrastructure of UIDAI consists of all technology components that are critical to establishment and continuity of UIDAI's core services such as identity, authentication and facilitation services. These technology components along with associated operating processes/procedures and people have specific risk profiles that need to be mitigated comprehensively and effectively. High level security components are listed below:

- i. **Data repository (CIDR):** CIDR essentially contains information that UIDAI intends to store and retain. This data store consists of various records such as UID numbers, demographic data, biometric data, enrolment records, updation records, authentication records, ecosystem information etc. Since this repository contains information that is of paramount importance to identify a resident and establish trail of events specific to a UID record, it needs to be protected at every stage of its lifecycle.
- ii. **Process automation components:** Authentication and enrollment servers are the two key components that fall in this category.
- iii. **Network security components:** Devices/products/solutions to provide secure storage, processing and transmission environment in the UIDAI data network. This could include controls such as firewall, anti-malware, encryption, logical access control etc.
- iv. **Key Management:** Key management is crucial to success of identity and authentication services for all stakeholders other than residents. It helps in establishing identity. Confidentiality/ integrity and ensures in non-repudiation of system users.
- v. **Application security:** Applications would act as the interface for information exchange so security of the presentation layer, application logic layer and the database layer needs to be considered.
- vi. **Logging and auditing:** Logs provide useful information to support troubleshooting, forensics, audits, trend analysis, internal investigations, incident response and optimizing system and network performance. It is essential that UIDAI collects, periodically reviews, and securely archives the security log data for a defined period of time.
- vii. **IT Support systems:** These are systems that provide either additional controls or facilitate security and IT automation assurance to the overall IT environment in UIDAI.

7.5.3. Defence in Depth

- i. UIDAI would adopt a defence in depth strategy to provide multiple layers of defence to safeguard the UID system. This approach ensures relevant controls are implemented in the key areas including people, technology and process (operations) to secure the UID system and the accompanying environment.
- ii. Some of the salient features of the UIDAI's security model include:
 - a. Connectivity to the UID application for UID enrolment and authentication (Private Portal) would be provided only for agencies that have been previously verified and authorized by UIDAI.
 - b. All operations affecting the resident's UID data including enrolment and updation would be carried out only with the resident's biometric data.
 - c. The technology stack at the CIDR (Central ID Data Repository) will be supplemented with appropriate security controls including firewalls, IPS (Intrusion Prevention Systems), etc. Additionally UIDAI may mandate similar controls for the agencies involved with the UIDAI system.
 - d. UIDAI's process and technology at CIDR would be standardized as per international security standards e.g. IS027001.
 - e. The UID application and the client libraries developed at the agencies involve security controls to mitigate against all risks example as specified in the OWASP (Open Web Application Security Project) or top 10 flaws.
 - f. UIDAI may conduct process audits of the information that comes in from the Registrars, to ensure data quality and that agencies are following guidelines recommended by the UIDAI.
 - g. UIDAI may propose stronger security controls for agencies involved in collecting and storing resident's supporting documents for obtaining the UID. These include electronic documents of resident's passport, ration card, voter's card, etc.
 - h. Personnel handling the information systems of the UID system have prior experience and are trained to safeguard the IT assets against risks.
- iii. As part of the envisaged Security Model, UIDAI requires GRCP-SP to monitor and provide assurance on Information Security, Privacy risks and Performance Assurance Services.
- iv. While Privacy is considered to be the key security requirement of the UIDAI system, other factors (Availability, Integrity, Authentication and non-Repudiation) governing the security of the UIDAI system should also be given par importance to ensure a safe and secure UIDAI environment.
- v. GRCP-SP shall ensure that the security model adopted by UIDAI addresses all these elements adequately at all layers (People, Process and Technology).

7.5.4. Collaborative Security Model

- i. Working in a partnership model requires security to be met at each of the involved parties to provide an end to end security of the UID system. While security implementation for the CIDR (Central ID Data Repository) will be the responsibility of the UIDAI / MSP, security of the UID connecting environment (application, networks, processes, etc.) at each of the involved parties would be taken care of the respective ecosystem partner.
- ii. UIDAI would provide a governing model of security involving technology and processes to each of the partners participating in the UID system. All UID data deemed to be private and sensitive in nature would be provided adequate protection while in transit and storage both at UIDAI and at the agents involved with the system.
- iii. The GRCP-SP is required to establish, implement and operationalise a framework to provide Governance, Risk, Compliance and Performance Assurance (GRCP) services to address security and privacy risks and provide SLA Process Assurance of UIDAI ecosystem partners.

Part 2: Governance, Risk, Compliance Framework and Performance Assurance Services

8. Need and Objective of IT Security Governance, Risk, Compliance and Performance Assurance (GRCP)

The vision of GRCP service provider (GRCP-SP) is to facilitate creation of a robust, comprehensive, secure environment for UIDAI to operate.

The overall goals of the GRCP-SP will be to:

- Design and implement a framework which can be used to establish sound foundational principles for information risk management in the UIDAI ecosystem through the use of relevant standards, frameworks and tools.
- Ensure implementation of Information risk management to meet the needs of UIDAI specific business environment and level of risk management maturity.
- Monitor and provide assurance on Information Security, Privacy risks and Performance Assurance Services

To achieve these goals the GRCP-SP shall provide UIDAI management with oversight of UIDAI and partner ecosystem in terms of (1) Visibility (2) Effectiveness and (3) Control. GRCP-SP is expected to measure, monitor and validate that all the ecosystem partners are adhering to the defined UIDAI IS policy and adhere to policy updates as and when released.

9. AADHAAR - Governance, Risk, Compliance and Performance Assurance (GRCP) Framework

UIDAI has complex assemblages of technology (i.e., hardware, software, and firmware), processes, a large ecosystem of services and people, working together to process, store, and transmit information in a timely manner to support its various operations and service delivery mechanisms. The immense degree to which UIDAI depends upon information systems indicates that the protection of the underlying Processes and systems is paramount to its success. As UIDAI would handle critical information of residents, it is imperative that the Infrastructure, applications, connectivity of and within UIDAI and its ecosystem are secure and that security related policies, processes and procedures are envisioned and implemented properly, as per standards specified in the UIDAI IS Policy.

Based on the UIDAI IS Policy, a GRCP framework needs to be designed and implemented that incorporates controls which are both managerial and operational in nature, and safeguards along with countermeasures to protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of the system and its information. The GRCP framework shall also incorporate appropriate mechanisms to manage Fraud Risks within UIDAI ecosystem.

Further to provide continuous oversight support for managing Information Security, Privacy risks in accordance with its business requirements, laws and regulations, the GRCP framework needs to provide implementation tools including policies, processes, procedures, guidelines, standards, forms and templates.

Due to its broadly integrated nature, the GRCP framework should consider multiple layers: These layers being hierarchical in nature shall cover all the elements of “Process – User – System”.

- **Business Process Controls Layer which** is the key driver for identifying all applicable risks and shall be the primary consideration in designing the GRCP Framework and implementation.
- **Identity Layer** which facilitates the relationship between users and business processes and must reflect and maintain the integrity of the Business Process Controls.
- **Infrastructure Security Layer which** is the underlying element in the hierarchy which shall serve to support the Business Process/User relationship - Considering the fact that an infrastructure setup that is unsecured would compromise the entire structure.

This integration should be expressed in terms of an **Integrated Governance Framework** that can be applied consistently across the UIDAI ecosystem – providing the appropriate balance between enablement and protection.

A comprehensive and systematic approach will help UIDAI to identify events and measure, prioritize and respond to the risks challenging its most critical objectives, initiatives and day-to-day operations.

Appropriate internal governance and management of risk and compliance is one of the key responsibilities of the GRCP-SP. UIDAI proposes to understand and categorize the information security and performance assurance under the GRCP framework (G-Governance, R-Risk, C-Compliance and P-Performance). These shall be defined and based on the core principles of security, privacy, compliance, comprehensiveness and accuracy and identified areas of deliverables under each of the pillars of this framework outlined below.

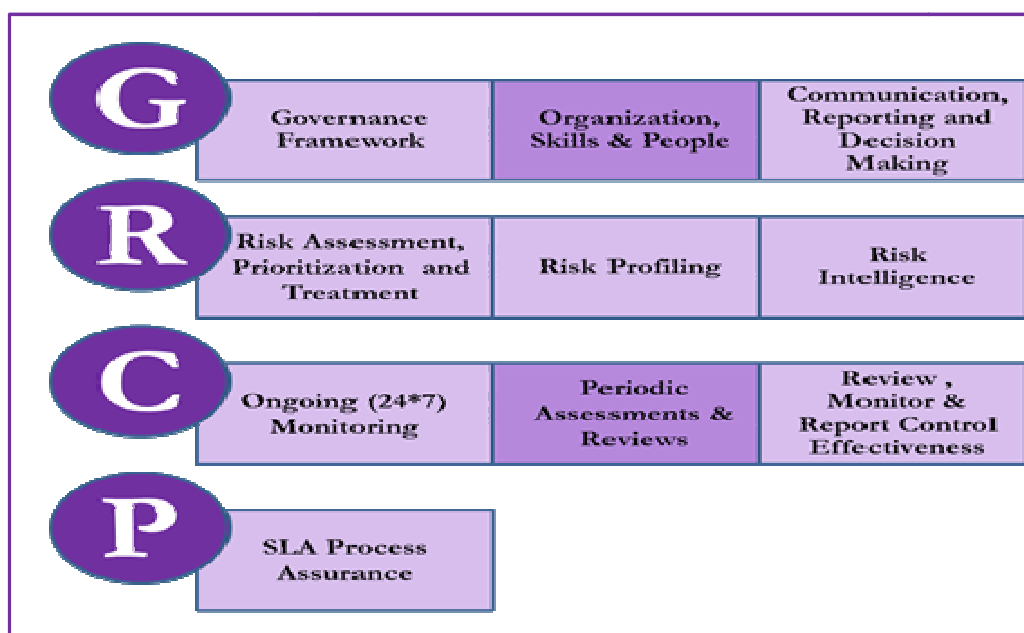


Figure 20: Overview of GRCP Framework

The indicative GRCP Operations View is outlined below:

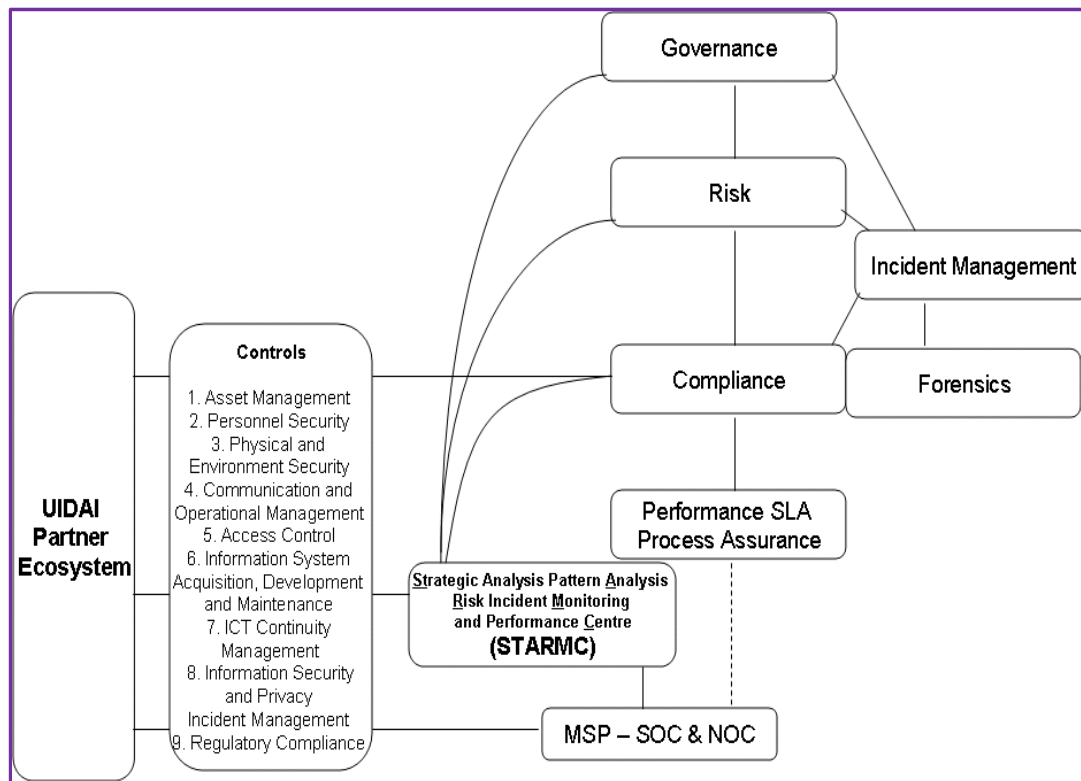


Figure 21: GRCP Operations View (Suggestive)

Needless to say the governance, risk, compliance and performance assurance (GRCP) framework and its effective implementation is very critical. This framework shall provide overall strategy, governance model and compliance framework to provide requisite oversight of UIDAI functioning. As the UIDAI grows, the complexity around creating a program to manage and protect associated information and/or assets and the propensity to commit a fraud will increase and hence the challenges of determining and maintaining compliance with multiple standards will be more.

While the ecosystem partners shall be responsible for implementing measures for effective information security and manage fraud risk, the GRCP Service Provider will be responsible to monitor and provide oversight support to UIDAI to ensure that all the ecosystem partners adhere to these requirements.

As part of the effort to develop GRCP framework, the GRCP-SP should gain an in-depth understanding of the scope of work to mitigate the threats and frauds by:

- Understanding the scope of work of the various ecosystem partners
- Understanding the business processes, functions, roles and responsibilities of various stakeholders

- c. Studying the UIDAI policy guidelines, architecture, design and the services envisaged
- d. Studying the SLA's between different stakeholders

The matrix provided here depicts the primary, secondary and tertiary work responsibilities and also an indication for the GRCP-SP as to where it could obtain the desired information for carrying out its activities.

Functionality	UIDAI Eco System	Primary	Secondary	Tertiary
Registration	Registrars	Registrar	GRCP	UIDAI
Biometric solutions	Biometric Solution Providers	MSP ecosystem partner /	GRCP	UIDAI
Enrollment	Enrollment Agencies	Enrollment Agency	Registrar / UIDAI	GRCP /UIDAI
Authentication	Authentication User Agencies	AUA	ASA / MSP / ecosystem partner	GRCP / UIDAI
Authentication	Authentication Service Agencies	ASA	MSP ecosystem partner /	GRCP /UIDAI
Training	Training Agency / CDA	Training Agency / CDA	MSP ecosystem partner /	GRCP /UIDAI
Testing and certification services	Testing and Certification Agency Including Device Certification	Testing and Certification Agency	MSP ecosystem partner /	GRCP /UIDAI
Logistics Services	Logistics Service Provider	DoP / TCIL / Others	MSP ecosystem partner /	GRCP /UIDAI
Contact Centre Operations	Contact Centre Service Provider	Contact Center	MSP ecosystem partner /	GRCP /UIDAI
Application Services	Application Software Development Maintenance and Support Agency (ASDMSA)	MSP ecosystem partner /	GRCP	UIDAI
Data Centre Site Operations	Data Center Service Provider	DCSP	MSP ecosystem partner /	GRCP /UIDAI
Data Centre Technology Operations	Data center Operator/ MSP	MSP ecosystem partner /	GRCP	UIDAI

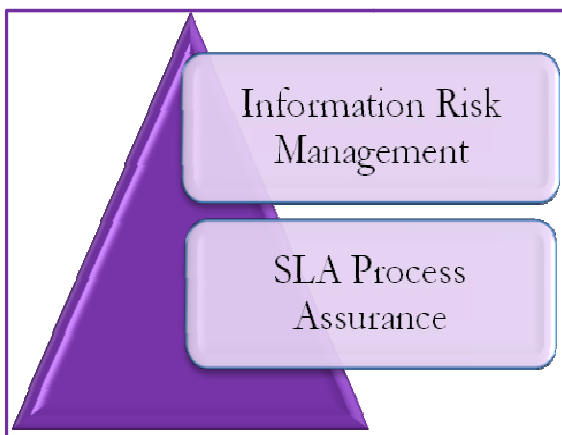
As the threat and fraud environment continues to grow with sophisticated and targeted attacks, it is important for the GRCP-SP to continuously and proactively track and mitigate these before they impact the UIDAI operations.

The GRCP-SP shall be successful in achieving its objectives only if it works in a collaborative and partnership model with the other UIDAI ecosystem partners and ensuring that they succeed in their respective responsibilities and obligations to UIDAI.

Indicative list of the threats and frauds

envisaged: Biometric Interception, Tampering Biometric Hardware, Fake Biometric Nodes, Infrastructure Node Impersonation, Inadvertent leakage, Registrar with Malicious intent, Fake Biometrics, Insider attacks, Enrolling false personal data, Denial of Service on CIDR, Unauthorized Query , Corrupt Signature verification, Corrupt Insider in central register, Privilege escalation, Service Spoofing, Intersection attacks. , Query Flooding, Printing fraud, Vulnerable computing devices (Unpatched and misconfigured systems, Bot command and control, Rootkits, Malware; Virus , Trojans, Keyloggers), Vulnerable applications (Cross site scripting, Buffer overflow, SQL injection , Denial of service, Defacement, Backdoors), Identity theft (Thru phishing, pharming, trojans, social engineering, Spoofing, Privilege escalation), Unauthorized access, Data leakage, Advanced persistent threats, Product backdoors, UIDAI infrastructure sabotage.

Functional Scope for GRCP-SP:



From the functional scope point of view GRCP – SP is expected to provide Oversight support to UIDAI on the Information Security and PrivacyRisk Management for the entire UIDAI ecosystem and provide assurance on the ecosystem partner SLA management. Such assurance shall be limited to validation of overall SLAmeasurement process of the Ecosystem Partners.

Figure 22: Function Scope for GRCP

Information Risk Management:

The fundamental precept of the UIDAI information security policy is to support its mission from the exposed uncertainties. Managing uncertainties is a daunting task because of the limited resources and an ever-changing landscape of threats and vulnerabilities. Therefore, UIDAI expects the GRCP-SP to bring in comprehensive information risk management to facilitate in sharing a commonly understood view of both IT and business concerning the potential impact of various IT security related threats to the mission.

Information Risk Management is envisaged as the process that allows UIDAI to balance the operational and economic costs of protective measures, should help the management identify appropriate controls for providing the mission-essential security capabilities and achieve gains in mission capability by protecting its IT systems and data that support the mission objectives. It involves understanding and responding to risks associated with and factors that may lead to a failure in the confidentiality, integrity or availability.

Information Risk Management comprises of understanding and prioritizing risk, developing risk mitigation strategies, effectively communicating, planning of the implementation and following up till closure to reduce the risk in a consistent and repeatable fashion to an acceptable level for an acceptable cost.

SLA Process Reviews:

SLA Process Reviews are driven by a desire to ensure increased control over the various ecosystem service providers to ensure and validate their compliance towards meeting the respective SLAs. Every ecosystem partner is responsible for measuring its own SLAs and furnishing detailed reports on a defined periodic basis. The measurement processes may vary from one ecosystem partner to another.

Broadly, GRCP-SP is expected to validate the current SLA measurement processes and tools with respect to their efficacy in measurement, frequency, cost-effectiveness and report on their final impact on the overall SLA management. GRCP-SP should also make suggestions based on the global leading practices to further optimize the existing processes wherever possible.

Overall Scope for GRCP-SP:

The overall scope of work has been developed around the “UIDAI GRCP” framework which covers and logically classifies various components under this framework.

Under this RFP, the Overall Scope for GRCP – SP is broadly distributed into the following two areas...

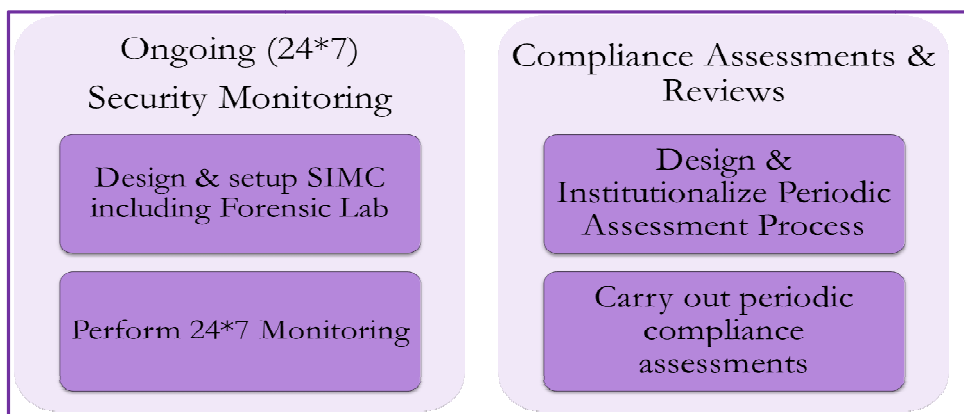


Figure 23: Overall Scope for GRCP

The above elements have been detailed along with the deliverables in the subsequent sections.

10. Scope for GRCP-SP

The elements of scope can be understood under the following four tracks:

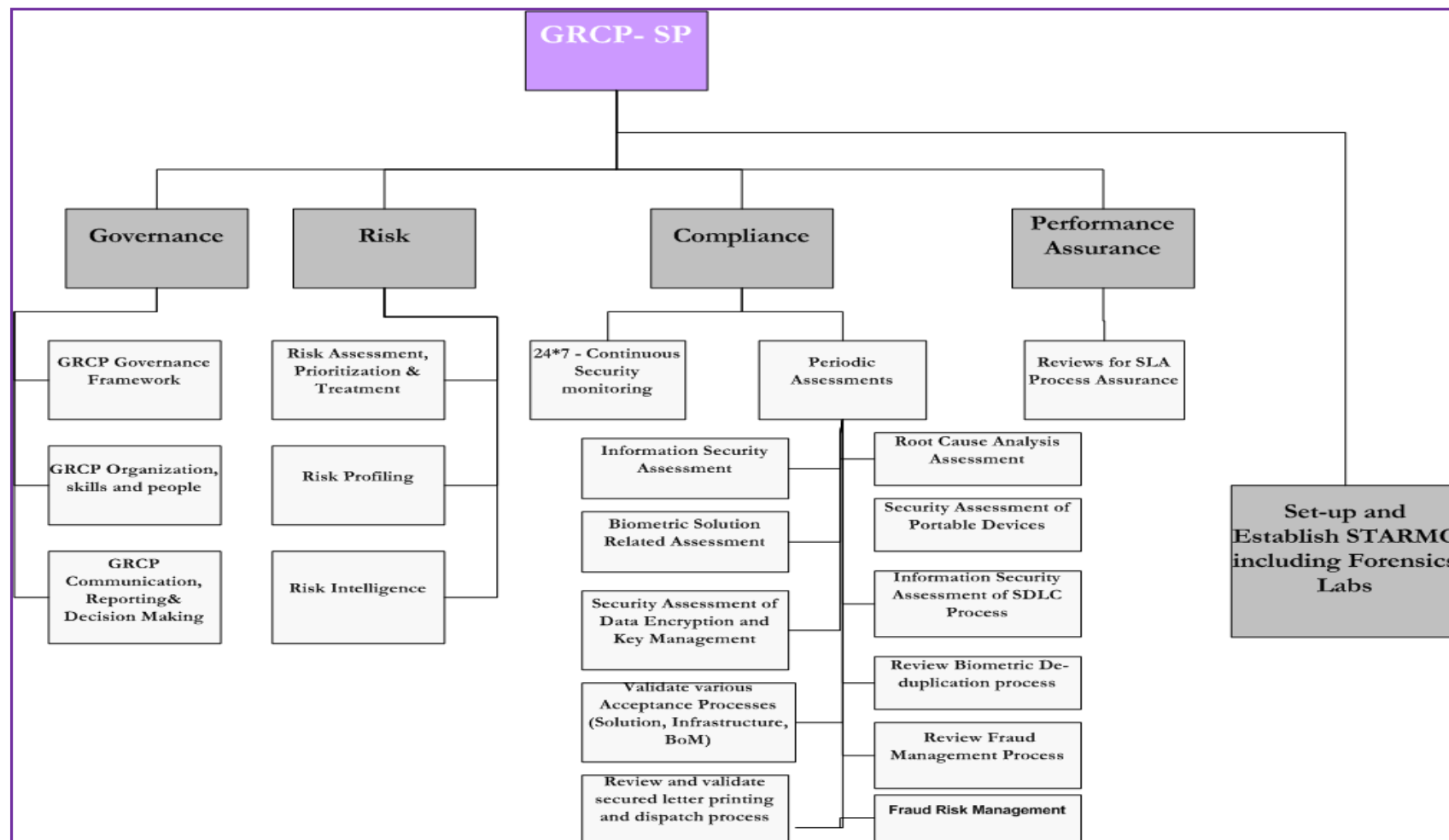


Figure 24: Overall Scope of Work for GRCP-SP

10.1. Governance

The overall objective of Governance would be to provide UIDAI management with information security and privacy visibility, effectiveness and control across UIDAI and its partner ecosystem.

It is expected that the GRCP Governance framework, structure, processes and the executive support systems shall facilitate and drive strategic alignment of information security with business strategy to support UIDAI objectives.

Establishing the governance structure and process should be done by identifying appropriate UIDAI and GRCP-SP representatives who will jointly make decisions and be held accountable. The joint (UIDAI and GRCP-SP) team would report into an executive / steering committee constituted by UIDAI having members from other Government Agencies including CERT-India.

10.1.1. GRCP Governance Framework

Objective

UIDAI requires a comprehensive framework that will provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

GRCP-SP will be required to define and design strategy, roles and responsibilities, policies, processes, procedures and frameworks to meet UIDAI objectives and aligned to the global leading practices and standards.

Overview of Scope

The governance mechanism is intended to help align Information Risk Management with the business through an integrated review and decision-making process which is aligned with actions for achieving overall business and strategic goals. This process shall also ensure that risk tolerance is continuously factored as per the UIDAI requirements and provides a way to set controls that can be assessed through an effective compliance process.

The outcomes of governance activities ultimately will define how effectively the overall Information Security, Privacy and Fraud Risk Management is designed and implemented throughout the UIDAI ecosystem.

The process to establish GRCP governance framework shall include the following activities:

- **Setting vision:** The GRCP-SP is expected to set a vision that will not only align itself with the Strategic Objectives of UIDAI, but also capture and articulate the benefits and contributions it will bring on to UIDAI ecosystem
- **Aligning GRCP Governance Framework with overall UIDAI Governance:** Design a comprehensive governance framework that will ensure a tighter fit and coordination between Information Risk Management Practices, GRCP governance mechanisms and overall UIDAI program governance.
- **Identifying regulations and standards:** Applicable requirements and standards play a critical role in gauging the exactness and rigor required for the overall success of GRCP function.
- **Assessment:** A comprehensive Risk Assessment to cover the areas of Information Security, Privacy and Fraud risks is expected to be performed as part of the design phase to establish the “foundation” – on which the short-term, medium-term and long-term GRCP roadmap for UIDAI will be built upon. This is expected to be performed based on UIDAI specific requirements and against leading practices such as ISO 27001, BS 25777, PCI DSS, Privacy, etc.
- **Policy Design:** Design / Augment the information security policy that will provide the updated version of baseline policy and controls that will be implemented across UIDAI ecosystem.

As part of “Governance” GRCP-SP shall ensure that the below requirements are appropriately addressed and incorporated

- Review and gap assessment of current protection strategies, Information Security policies, practices and tools.
- Review and gap assessment of current IT and Security Infrastructure deployed by UIDAI / MSP / Ecosystem partners
- Prevention, monitoring and handling of fraud in terms of robust policies, controls and procedures
- Submit benchmarks of overall GRCP effectiveness to UIDAI against similar operations / organizations in India and globally
- Identify, map and document compliance and regulatory requirements
- Maintain trends and indicators for UIDAI system resilience

- Map key risk indicators to key business performance indicators and establish and maintain a strategic risk index for the entire UIDAI ecosystem

Deliverables *(inclusive but not limited to)*

1. GRCP Vision Document
2. GRCP Framework and Program Design / Strategy (To be developed one time as part of the design phase and reviewed and updated on an annual basis subsequently)
3. Initial Risk Assessment / GAP Report
4. Updated version of Baseline Information Security Policy for GRCP ecosystem

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

5. **Strategic analysis report** (This report should provide scenarios of threat analysis and response based on international and domestic events that can threaten and impact UIDAI. It should assess how risk is shared among ecosystem participants and also determine the best strategies to protect them. Both threats (intention and capabilities) and risks (probability and consequences) must be considered in the formulation of strategy presented in the report to UIDAI. It should cover analysis of the security and privacy industry, analysis of national identity, provide strategic description, strategic evaluation, strategic issues that need to be addressed and strategic recommendations to UIDAI)

10.1.2. GRCP Organization, skills and people**Objective**

It is critical for UIDAI program that an expert information risk management group is established and managed on an ongoing basis by the GRCP-SP. In line with the core objectives of this RFP, UIDAI requires full time, dedicated resources providing information security and SLA Process Assurance to the UIDAI ecosystem by the GRCP-SP.

Overview of Scope

GRCP-SP would be responsible for setting up and maintaining GRCP office. GRCP-SP needs to propose an organization structure which will be under the direct supervision of UIDAI Executive Committee. GRCP-SP will deploy a team of dedicated resources on-site with the required skill sets to effectively carry out the activities as identified in this RFP. GRCP-SP will have to clearly define the roles and responsibilities of each team member.

While this RFP will mandate a minimum set of team members along with the required skill set, the GRCP-SPs expected to propose (as part of response to RFP) an optimal Organization Structure (along with number of team members and profiles) and necessary automation and tools that are deemed adequate for successful service delivery of the project.

Key Activities

- Identify the functions / activities that the members of GRCP-SP team will perform
- Define the role of each individual with respect to overall Information Security, Privacy and Fraud Risk Management
- The proposed Organization Structure shall be finalized in consultation with UIDAI and the same shall be institutionalized.
- Identify and recommend the roles of both entities (UIDAI and GRCP-SP) and other organizational structures that need to be institutionalized.
- Advise UIDAI in formation of UIDAI Executive Committee which shall provide overall direction and decisions to GRCP-SP

Deliverables *(inclusive but not limited to)*

6. Finalized GRCP Organization Structure and deployment plan.
7. Finalized Job Definitions and Specifications;
8. Finalized Roles, Profiles and User Assignment.
9. Performance Measures for all KEY profiles;

The bidder needs to provide the details of proposed Team Members as per the requirement of this RFP.

10.1.3. GRCP Communication, Reporting & Decision Making**Objective**

The objective of setting up a pre-defined communication and escalation channel is to ensure that the issues are effectively and adequately communicated and escalated to the concerned ecosystem partner or to UIDAI according to their severities and ensure that appropriate and timely decisions are taken.

Effective reporting and maintaining a unified view for the plethora of activities performed and analyses and assessments done, becomes highly crucial for the core decision makers to focus and act on the required aspects. Hence, a standard reporting system has to be

established to have clear and redundancy free reporting and mechanisms to maintain and provide a unified view of UIDAI ecosystem from a GRCP point of view.

Overview of Scope

In order to ensure that an effective communication and escalation is done to the concerned ecosystem partner or to UIDAI, GRCP-SP needs to define a proper communication and escalation process flow throughout the UIDAI ecosystem.

GRCP-SP should also design reporting standards to be used in every assessment, analysis and monitoring activity being furnished at any point in the complete GRCP sphere. Also, it needs to design mechanisms and techniques to maintain a unified view of the overall activities and outcomes so as to facilitate proper decision making.

Key Activities

- **GRCP Communication:** Recognizing the complexity in a setup such as UIDAI where there are multiple partners coexisting, the GRCP-SP is expected to establish a communication process that is simple but provides an efficient and effective flow of information amongst all the stakeholders. The GRCP-SP shall assess the reporting requirements w.r.t each stakeholder and institutionalize a process that incorporates efficient use of technology to build effective communications system.
- **Design and Implement Executive Support System:** With a primary objective of supporting UIDAI senior management in its decision making process, GRCP-SP shall implement the following dashboards and institutionalize a process through which the GRCP-SP can provide the UIDAI with relevant inputs and insights that support in effective decision making.
 - **Executive Risk Dashboard:** Effective information security cannot be achieved through single, point-in-time security assessments. Rather, to achieve true security, it is paramount that GRCP-SP implements a strategic and an executive risk dashboard which incorporates risks related to people, processes, and technology across UIDAI ecosystem and to employ appropriate measurements to manage and improve risk management program effectiveness on a continual basis. *The Executive Dashboard is expected to provide inputs for the purpose of Decision Making to the senior management of UIDAI and other high level committees as need be.* Hence the inputs are required to be in the form of business language relevant to UIDAI.

- **Compliance Dashboard:** Based on the overall GRCP framework, GRCP-SP is required to establish a program to ensure that UIDAI partners are adhering to overall Information Security, Privacy and Fraud Risk Management requirements. Consolidating this information and gaining both a comprehensive and comparative view of partner compliance is critical to the ongoing management of overall UIDAI risks. It is expected that GRCP-SP would setup and maintain a compliance dashboard system to drive the same.
- **Define Report Standards:** Identifying key stakeholders within UIDAI ecosystem, the GRCP-SP shall determine key reporting requirements, the type and frequency of reporting, etc. The GRCP-SP Shall also design and automate the report formats. The GRCP-SP shall ensure adherence to defined SLAs for all reporting requirements.
- **Establish robust Escalation Procedures** that clearly identifies the Escalation Activity, Escalation Chain and Hierarchy, Responsibility and Action Items. Robust escalation procedures play a critical role in ensuring high quality of an incident response. Since security incident management is essentially a problem management activity, there must be clearly defined integration points with the overall UIDAI problem management and disaster recovery / business continuity processes.

The service provider shall also appropriately consider and incorporate the following UIDAI requirements as part of their proposal.

- Decision making process flows between the GRCP team and UIDAI ecosystem partners
- Support for technical and non-technical communication during incidents for UIDAI senior management for dissemination to government and public
- Relationships with external vendors, CERT-In, Researchers and all UIDAI ecosystem partners
- GRCP related communication for Government and Parliamentary Questions. Respond to audit and government queries related to governance, risk, compliance, performance around security and privacy
- Create and Maintain a data repository as needed for UIDAI decision making
- Develop, update and test incident response plans and crisis communication plans
- Templates for reports to be submitted by various service providers for Risk, Compliance, Performance and Incident Management and also templates for reports to be submitted by the GRCP-SP to UIDAI.
- Maintain metrics on critical incidents – percentage of incidents detected by internal controls, incidents that are preventable, incidents avoided, and type/number/severity/location of incidents, mean time between incidents, mean time for discovery, and mean time for closure.

- Establish and maintain financial impact per incident, down time due to incident, resolution person hour per incident
- Help UIDAI make risk aware decisions by providing analysis, recommendations and solutions for avoiding risk, accepting risk, transferring risk and mitigating risk

NOTE: The service provider is expected to provide the approach and methodology for delivering the above components as part of their technical proposal.

Deliverables (inclusive but not limited to)

10. Finalized Communications Plan & System Requirements
11. Finalized Reporting Standards including the mechanisms, formats and automation requirements
12. Finalized Executive Support System incorporating Executive & Compliance Dashboards
13. Finalize and Implement Escalation Procedures

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

14. **Incident related metrics** (such as - Average time to fix an incident, Percentage of Incidents Resolved at First Level such as Eco system partners or MSP, incidents due to SLA Violations, Source of Incident Detection (User, Monitoring tool, etc.), Chances of incident reoccurrence, number of incidents that could not be simulated, Incident Fix type (Permanent fix, workaround), number or percentage of incidents converted into Problems, discovery of potential incident situation numbers, Open incidents by – partner ecosystem, process, technology, time it is open, expected time to closure, business impact, criticality)
15. **Resilience trends and metrics** (such as - the average time elapsed until service restoration after an incident, number and duration of incidents with impact on the network / service unavailability, the number of failure points that result in various levels (40%, 50%, 75%, 80%) of loss of availability, confidence factor that risks from all sources that need to be identified have been identified, probability of delivering a service through a disruptive event, for disrupted high-value services with a service continuity plan the percentage of services that did not deliver service as intended throughout the disruptive event, percentage of high-value assets and services with controls that are ineffective or inadequate, an ideal situation for resilience shall be that no security / privacy incidents or breaches occur or there is no loss of Confidentiality, Integrity or Availability in any service, arrive at trends using statistical models such as - regression models for recognizing trends, using cluster analysis, time series analysis, etc.)

16. **Regulatory compliance progress** (such as – percentage of activities completed against those planned, design and operational deficiency status report, process heat maps, assessment progress, remediation progress, internal audit progress, percentage of completion of self-assessments based on predefined templates, percentage of ISO 27001 controls implemented for a particular system / service / organizational unit, number of outstanding audit actions, etc.)
17. **GRCP benchmark metrics** (such as – benchmarks for: GRCP strategy, investigations, managing information (privacy, security, etc.), enabling technology, effective risk assessments, percentage of automation controls used for internal security and regulatory policy compliance, etc.)
18. **Security maturity and performance of service reports** (such as - optimized, managed, defined, repeatable, initial / new for the various domains; number of incidents / breaches causing outages and length of outages over a given period service wise; etc.)
19. **Process maturity metrics and maturity index** (such as - optimized, managed, defined, repeatable, initial / new for the various processes; developing an overall maturity index score)

10.2. Risk

Risk in the context of UIDAI may refer to any systematic or sporadic event or trigger that could cause the program to fail or achieve its objectives within the stipulated time period, cost or operational constraints. In order to maintain an updated and comprehensive risk mitigation plan, it is imperative to assess any exposure of UIDAI to any potential risk or vulnerability.

The final outcome expected from the GRCP-SP for Risk shall be to provide UIDAI management with Specific, Measurable, Accurate, Reliable and Timely (SMART) metrics on reducing risk for UIDAI, increasing information security and risk awareness across the ecosystem and a Risk index as a measure of progress being made.

Information technology plays a critical role as part of the UIDAI business operations. Precisely because of its crucial role and the complexity of partners and processes involved, IT also exposes UIDAI to high levels of risk raising valid concerns in the overall risk posed to Information Assets in UIDAI such as

- Are there hidden risks that could undermine the whole UIDAI ecosystem?
- Whether, appropriate controls have been designed and implemented?
- Is the structure and staffing planned sufficient to meet evolving needs?

The overall objective of Risk shall be to provide a unified view of risk, pattern analysis, attempts of fraud, internal threats and external threats inputs by identifying, analyzing, visualizing, managing, communicating, and protecting UIDAI from threats and collaborating with the various stake holders across UIDAI. As part of the Risk framework, the GRCP service provider shall be responsible for the following:

10.2.1. Risk Assessment, Prioritization & Treatment

Objective

Risks in UIDAI context could be any event which may cause a disruption in availability or quality of services offered such as Enrolment/Authentication. Each UIDAI ecosystem partner brings in a certain set of risks into the overall solution. Accurate risk identification becomes a crucial step in developing risk mitigation strategies. It is also instrumental in making the stakeholders visualize the risks involved in the UIDAI ecosystem.

Overview of Scope

The GRCP-SP will need to assess risk within the UIDAI ecosystem. The results should guide and determine the appropriate management action and priorities for managing information security and privacy risks and for implementing controls selected to protect against these risks. GRCP-SP will also develop and drive risk treatment plan that will mitigate risks within the ecosystem. For those risks where the risk treatment decision is to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by risk assessment.

GRCP-SP should carry out a structured process to determine the criticality and sensitivity of the information being processed, stored, and transmitted by all the UIDAI ecosystem partners. This would ensure performing an information risk assessment for the complete UIDAI ecosystem including cloud to evaluate the possible threats and their respective probabilities. The assessment should be reported and identified risks should be stored in a 'risk register' which is a central repository for maintaining all known risks.

Key Activities

Given the significance the GRCP-SP shall ensure that the overall stature of internal control to support the required level of security and compliance by taking up the following activities:

- Undertake a risk assessment to assess the current state for identifying the key risk associated with critical information assets associated with business and IT processes of all UIDAI ecosystem partners
- Assess the current level of controls already implemented

- Perform a gap analysis between the required and current level of controls
- Define Risk mitigation plan / 'Risk Treatment Plan' by prioritizing, evaluating and implementing appropriate controls. The GRCP-SP shall establish Acceptable Risk by interacting with the various stakeholders. The mitigation plan shall suggest any policy level changes, new tools and products, technology architecture changes etc. which may be required to mitigate the identified risk.
- Track and monitor risk treatment plan and facilitate their closure as a primary responsibility.
- Considering the Mitigation Plan and existing residual risk, define Risk Acceptance Criteria. Develop procedures which may be required as a part of mitigation steps.
- Perform a gap analysis with respect to the tools proposed and deployed by MSP/ecosystem partner vis-à-vis information security.

GRCP-SP as part of this exercise is required to perform on the ground assessment at the ecosystem partner's physical locations/ sites as required to cover the information security, privacy and continuity risks.

As part of the Risk Assessment, Prioritization & Treatment exercise the GRCP service provider shall appropriately consider the following UIDAI requirements and incorporate the same in their technical proposal and deliverables.

- Identify the scope of risk analysis to be performed on the various ecosystem partners
- Undertake a detailed study of the business and IT processes of UIDAI and UIDAI ecosystem partners to understand the risks involved, threats and vulnerabilities and their impact
- Carry out a risk assessment for and provide assurance framework to include UIDAI cloud security, privacy and IT continuity risk
- Identify, analyze, categorize and prioritize risks for devices, services, software based on data collected and business impact on UIDAI
- Identify the threats for devices, services, software due to human errors, technical failures, deliberate acts, control deficiency and environmental considerations.
- Review various compliance and performance reports to identify risk and opportunity signals
- Update the risk register periodically with every risk identification exercise
- Ensure that the Risk Control Matrix at a minimum shall consider the aspects of control objective, control activity, responsible personnel, control type, control classification, test of design method, design effectiveness, justification of design assessment, test date, test method, control operating effectiveness conclusion, rationale for control operation, frequency of testing.

Deliverables *(inclusive but not limited to)*

1. **Information Risk Assessment report of the UIDAI ecosystem-** This deliverable is expected at the time of developing the first time GAP report in Governance Phase, and on an ongoing basis as per the approach and periodicity designed by GRCP-SP.

The first time report shall also cover risk assessment to review gaps of any security infrastructure of MSP/ ecosystem partners.

The report shall provide a detailed assessment of risks, threats and vulnerabilities associated with the business and IT processes of UIDAI and UIDAI ecosystem partners.

2. **Risk Analysis Scope document for ecosystem partners** - Document the scope of risk analysis to be performed on the various ecosystem partners on an on-going basis.
3. Develop and maintain a **Risk Register, Risk & Controls Matrix**
4. **Develop Risk Treatment Plan** which includes **Risk Mitigation Plan** and Acceptance Criteria. The Risk Treatment Plan shall be reviewed on a quarterly basis during the operational phase. Further, the Risk Treatment Plan shall be updated as and when needed based on risks identified during the operational phase. The Risk Treatment plan will also provide details regarding the assignment of owners/ecosystem partners for each identified risk.
5. **Unified Risk Index view** - Provide a single real time unified view for risk and a risk index of the UIDAI ecosystem with drill down to the component level
6. **Controls effectiveness, efficiency and maturity report** (example for malware - Control Effectiveness – average age of signature file on desktop – target days / actual days, status – red/green/yellow; control efficiency – number of persons required to support at UIDAI, numbers required in benchmark organization, status – red/green/yellow; maturity level of the control for malware – optimized, managed, defined, repeatable, initial / new; etc.)

10.2.2. Risk Profiling

Objective

Complex assemblages like UIDAI ecosystem would inherently have many information security risks and it becomes extremely difficult and resource intensive in attempting to mitigate all possible threats. Also, the nature and periodicity of compliance audits to be

performed on a certain control/process will depend upon its severity of risk. Thus, the risks need to be prioritized in a structured way based on their impacts so as to enable UIDAI in developing cost-effective risk mitigation strategies.

The primary objective of developing Risk Profiles for UIDAI ecosystem partners is to provide an acceptable security level for each of these partners and functional groups providing optimum Security Posture and compliance levels which shall lead to lower cost of operations.

The aim should be to develop an overall risk profile for the ecosystem partner and partner group that are reflective of the maturity and level of adherence to identified control requirements.

Overview of scope

Risk Profile in the context of UIDAI is extremely critical due to the varying nature of factors such as the business operations, size, complexity, and level of access to UIDAI infrastructure. These Risk Profiles are intended to assist UIDAI in ensuring effective oversight of information security of each of the ecosystem partners.

Key Activities

- GRCP-SP shall perform a detailed analysis of all the risks identified as a part of the Identification phase.
- The GRCP-SP should perform risk profiling (of ecosystem partners and functions) based on all the identified threats and their respective vulnerabilities and maintain a strategic risk index to help UIDAI in appropriate risk mitigation strategies.
- A priority matrix shall be prepared by the GRCP-SP detailing the impact and probability of occurrence of the risks. The risks priorities shall be updated to individual risk owners and the risk register.

Based on this exercise the GRCP-SP is expected to come up with a maturity rating for each of the processes and ecosystem partners.

Deliverables *(inclusive but not limited to)*

7. **Risk Profiles – Process / Function Wise / Eco System Partner Wise**
8. **Application and Infrastructure White-list** - Identify and publish “white-list” of applications and infrastructure – Process / Eco System Partner Wise

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

9. **Report on availability, confidentiality, and integrity of information risks** - GRCP-SP shall carry out and report on the risk assessment procedure for the suitability of the design of the controls, tests of controls and the results of the tests related to availability, process integrity and confidentiality including privacy.

10.2.3. Risk Intelligence: Initiatives to stay ahead of emerging Threat & Risk Profile

Objective

With the ever increasing functionality and complexity of UIDAI information systems and plethora of information security threats posing a hazard to sensitive information systems like UIDAI, it becomes imperative to be proactive in taking actions on future threats and stay ahead of the emerging risk curve.

Overview of Scope

In view of ever changing security landscape externally and changes in UIDAI's infrastructure (physical, network, systems, applications), changes in business/infrastructure processes and the related changes in compliance landscape, it is paramount that a security advisory and research group is established for providing expert security advise, conduct review and suggest best-practice recommendations to UIDAI on a regular and ongoing basis.

GRCP-SP should establish a capability to envisage on a proactive basis, the globally emerging information security threats and help UIDAI in aligning its future initiatives and missions to be free from information security and privacy risks. Through this capability, GRCP-SP shall help UIDAI make risk aware decisions by providing recommendations and solutions for avoiding, accepting, transferring and mitigating risks proactively.

Key Activities

- Develop a **Global risk intelligence feed / dashboard** with capability to ensure that UIDAI's infrastructure is secured against global threats and cyber-attacks. This risk dashboard should have global risk intelligence feed capability to ensure that UIDAI's infrastructure is secured against global threats and cyber-attacks.
- For ensuring security across an extended enterprise setup like that of Aadhaar, GRCP-SP shall interact with multiple state governments, public sector entities, international

security agencies, academic information security researchers, information security product vendors, CERT-IN and quasi-government organizations on a continuous basis..

- Create ability to provide deep visibility into ongoing vulnerability trends and data-points vis-à-vis global security risk and breaches which will help achieve the security solution for Aadhaar to be more holistic and relevant in a dynamically changing environment and evolving threat scenarios such as cyber-wars, mule-networks, bot-nets, and advanced persistent threats (APT), etc.
- Analyze risks based on future business strategies and directions that UIDAI plans to implement and recommend mitigation
- GRCP-SP should perform early warning analysis of new vulnerabilities, the latest cyber security threats and their impacts
- Simulate current and future threat scenarios and assess business impact on UIDAI in terms of confidentiality, integrity and availability
- Provide benchmarks (including fraud) to UIDAI against organizations in India and globally

Deliverables (*inclusive but not limited to*)

10. Design and Implement a Global risk intelligence feed dashboard
11. Expected future threats and risk mitigation plan reports
12. Threat exposure and forecast report – Based on the future threats and their mitigation plans the deliverable shall detail out the residual threat exposure and forecast on business impact. In cases where there is no mitigation plan for a future threat scenario, then the deliverable shall detail out the threat exposure and forecast on business impact.
13. Pattern analysis report
14. Trend report of category wise threats
15. Benchmark report of UIDAI against organizations in India and globally

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

16. **Report on threats by technology, severity, type and impact to UIDAI–GRCP-SP** shall use the consolidated and analyzed threat data, emerging threat data and shall monitor threats against specific devices and applications so as to provide informed reports on threats by technology, severity, type and impact to UIDAI.
17. **Weakest link reports for return on security investment–** GRCP-SP shall use the consolidated and analyzed threat data, vulnerability data, and emerging threat data and shall monitor threats against specific devices and applications so as to identify the weakest links in the security framework and architecture to suggest better allocation of security spending.

18. **Consistency reports for return on security investment**– GRCP-SP shall use the consolidated and analyzed threat data, vulnerability data, emerging threat data and shall monitor threats against specific devices and applications so as to identify the areas in the security framework and architecture which are consistent in the return on security investment and where security spending needs to be maintained.
19. **Efficiency reports for return on security investment**– GRCP-SP shall use the consolidated and analyzed threat data, vulnerability data, and emerging threat data and shall monitor threats against specific devices and applications so as to identify the areas in the security framework and architecture which are providing significant reduction in risk compared to the resources used.
20. **Opportunity report for return on security investment**– GRCP-SP shall use the consolidated and analyzed threat data, vulnerability data, and emerging threat data and shall monitor threats against specific devices and applications so as to identify the areas in the security framework and architecture where an opportunity exists for reduction in risk by security spending.

As part of the initiative to build Risk Intelligence the GRCP service provider shall appropriately consider the following UIDAI requirements and incorporate the same in their technical proposal and deliverables such as:

Infrastructure Requirements (indicative but not limited to)

- GRCP-SP shall deploy/use data feeds from the existing detectors and sensors, establish data feeds from external sources
- Ensure and identify minimum bandwidth, performance overhead on existing infrastructure and additional storage requirements, transmission and retention of data in encrypted form
- Infrastructure for risk simulation, risk rating and analytics

People and Skill Requirements

It is expected that the GRCP Service Provider shall staff adequately with individuals who possess relevant training and experience for carrying out Risk Profiling activities and show case the same as part of their technical proposal.

10.3. Compliance

The goal of this effort shall be to bring together the best practices in compliance management and establish a compliance program that provides oversight of the entire business operations of UIDAI. The GRCP-SP shall establish and implement the compliance program in line with the GRCP governance framework that will provide complete assurance that all UIDAI ecosystem partners and their processes are fully compliant with UIDAI IS policies, laws and regulations and protect the confidentiality, integrity (including non-repudiation and authenticity), and availability of UIDAI system and its information.

In line with the overall GRCP Framework, it is expected that the GRCP – SP shall enable the creation of single integrated and structured compliance architecture. GRCP – SP shall approach the compliance requirement more from a strategic perspective which could help UIDAI move beyond simply meeting individual compliance mandates to realize tangible business benefits.

The compliance architecture shall facilitate management of compliance initiative centrally and shall ensure adherence with multiple compliance requirements. The compliance architecture shall be designed in a manner that it should provide integrated compliance management and reduce the effort in coping with frequent changes in compliance requirements across multiple geographies, ecosystem partners and business processes.

As part of the compliance program, the GRCP-SP shall carry out Continuous (24*7) security assessment / monitoring and Periodic Assessments of UIDAI ecosystem processes and partners.

10.3.1. Design and Set up of Strategic Analysis and Risk Monitoring Center (STARMC) including Forensic Lab

Objective

The objective of setting up the STARMC is to identify, analyze, study trends, patterns and correct the incidents (security incidents/ fraud) that may have happened or have the potential to occur so as to prevent a future reoccurrence or occurrence. To meet this objective, the GRCP-SP would be required to setup and maintain a STARMC including a Forensics lab that will have the capability for event/log identification, management and correlation platform for monitoring events of devices, services, software at host, network and application level and for handling sensitive security events therein.

The objective of setting up a Forensics lab is to provide computer forensics support that has the ability to conduct both *reactive and proactive forensic investigations* including working with law enforcement agencies (lab must be equipped with tools to preserve, acquire computer evidence, analyse and present the same for investigation purposes).

STARMC guidance:

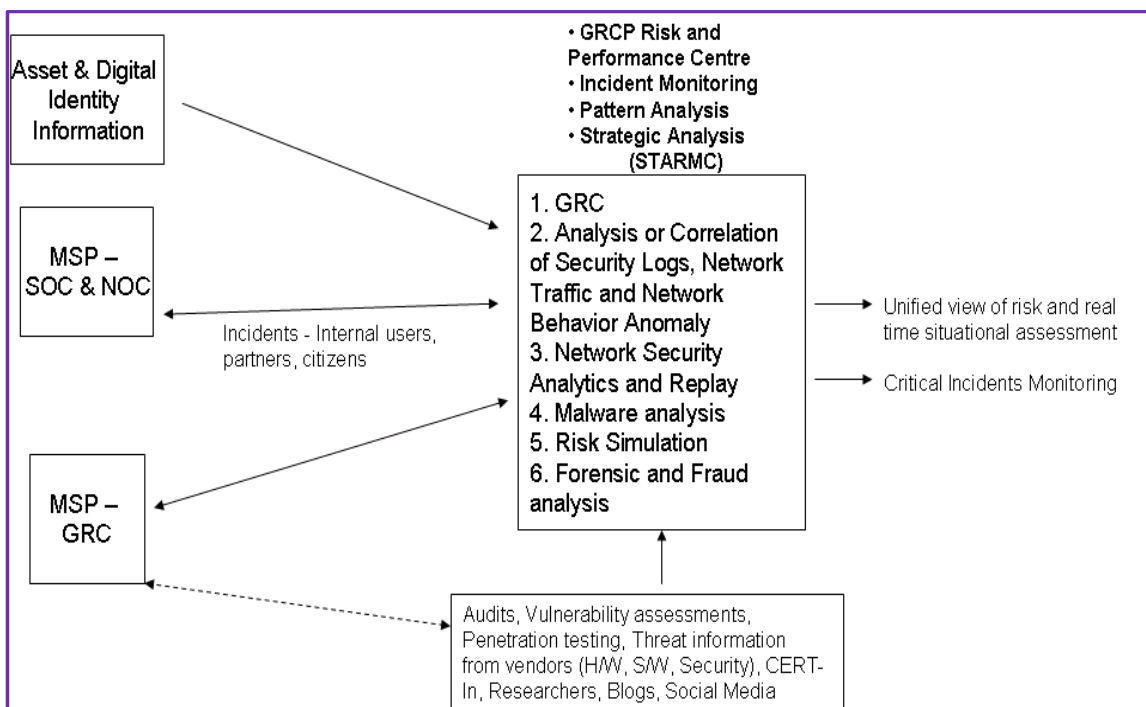


Figure 25: Guidance for STARMC

UIDAI shall provide the physical site for setting up the STARMC including forensics lab. The GRCP-SP shall be responsible for all site preparation activities and for setting up and establishing the STARMC including forensics lab.

Overview of Scope

Strategic Analysis and Risk Monitoring Center (STARMC)

- The GRCP-SP must implement and operate a Strategic Analysis and Risk Monitoring Center (STARMC) including Forensic Lab within the premises and setup provided by UIDAI. STARMC is required to monitor and manage states and events (of devices, services, software) at host, network and application level by correlating logs,

vulnerabilities, configurations, assets, performance and network behavioral anomaly data and collaborating with the ecosystem partners and other stakeholders across UIDAI.

- As part of STARMC, GRCP-SP shall setup and maintain a security event/log management and correlation and analysis platform for monitoring and analyzing various systems, devices, or applications events such as, firewall activity, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) activity, antivirus activity, Key Management Server and Authentication Servers, Routers, Switches Network and other Infrastructure Components.
- GRCP-SP is expected to access and use the feed from the detectors and sensors that are already implemented by UIDAI ecosystem partners. UIDAI will facilitate appropriate access to such tools and feeds to enable GRCP-SP to function effectively. The GRCP-SP shall identify the gaps in tools available with ecosystem partners and shall identify the additional tools required for effectively performing the **24*7 security monitoring and analysis function**. The GRCP-SP shall factor in such additional tools as part of its technical and commercial proposal. The GRCP-SP is required to propose and deploy all tools that are required for its effective continuous security monitoring, apart from those available with ecosystem partners including Database servers, application servers, web servers, client machines, etc.(Hardware and software).
- GRCP-SP shall deploy detectors and sensors or use data feeds from the existing detectors and sensors to **monitor** aspects such as patch management, PC security, secure remote administration, security policy management, transaction monitoring, user authentication, log management and analysis, configuration assessment, etc.
- It is expected that this would be achieved by setting up and maintaining detectors and sensors such as: anomaly detection, anti-virus, data security, enterprise security, web security, vulnerability detection, intrusion detection, malware detection, monitoring messaging security, identity, authentication and threat management.
- The Strategic Analysis and Risk Monitoring Center (STARMC) shall support workflows so that multiple experts from different domains can work on their respective views. It should be web based providing secure access from anywhere over the internet or intranet and should be scalable to incorporate new compliance standards and additional users as and when required.
- The GRCP-SP shall be responsible for Device Health Management, Patch Management, Change Management/ Capacity Management for STARMC Devices
- GRCP-SP shall also be responsible for designing and conducting security drills for confidence building in the overall UIDAI and ecosystem partner IT system and preparedness gap identification exercise from the perspective of response and recovery capabilities. In addition GRCP-SP shall mandatorily participate in all CERT-In conducted drills.

Forensics Lab:

- The GRCP-SP shall establish forensic policies and practices to address all security considerations as required for UIDAI. For this purpose, the GRCP-SP shall also co-ordinate with Legal advisors and law enforcement agencies (including CERT-In) to carefully review all forensic policy and high-level procedures and ensure these policies and practices are framed in line with UIDAI's IS policies, applicable laws and regulations.
- The GRCP-SP shall develop a forensic methodology to outline the proposed Investigation and Remediation Approach, Data, and Evidence Extraction and Storage, Analysis Methodologies and reporting the same under different conditions.
- The GRCP-SP is also required to ensure proper Investigation Completion and play a primary role in supporting UIDAI to ensure interactions, supply evidence as necessary and coordination with Law Enforcement Agencies as required.
- Forensics team shall advise ecosystem partners to follow procedures keeping forensics in consideration that may support Forensics team to efficiently and effectively perform forensics investigation.
- Providing training to key IT professionals in UIDAI to facilitate them in assisting investigations in an efficient manner

As part of setting up of Forensics Lab in STARMC, the GRCP service provider shall consider the following critical aspects and incorporate the same in their technical proposal and deliverables

- Multiple sources of data and evidence residing across multiple internal and external systems and technology infrastructure
- Critical pieces of data and evidence may be co-mingled with non-critical data requiring effort to separate the data components
- Deploy tools, technologies and software to enable Server Acquisition, Disk Forensics, Password Recovery, Steganography Investigation, etc.
- Design, maintain Fraud pattern definitions
- Actions taken to recover systems and gather facts so as not to destroy evidence
- The requirements of civil and criminal laws that need to be considered and in some cases across multiple legal jurisdictions
- Setting up checks and measures to prevent the unwarranted use of applying forensics to safeguard the confidentiality of the information

Key Activities

The STARMC including Forensics Lab will be responsible for providing the following services to the Aadhaar ecosystem:

- Design, Setup and operationalize STARMC and Forensics Lab along with their support systems and processes
- The GRCP-SP shall obtain acceptance approvals from UIDAI / agencies designated by UIDAI on the design and operational aspects of STARMC including Forensics Lab before going live.
- GRCP-SP shall be responsible for assisting UIDAI in the Acceptance process. Acceptance process is defined as
 - Commissioning and Demonstration of the applicability of utilization of individual Hardware/Software/Products/Tools in STARMC including the Forensic Lab and
 - Commissioning and Demonstration of the applicability of utilization of integrated STARMC as a complete solution
 - Institutionalizing and operationalizing the organization structure, systems and processes for effective STARMC operations
 - GRCP-SP shall obtain the Acceptance Sign-off on the above from UIDAI for Go-Live
- Establish roles and responsibilities of all the involved parties performing or assisting with the organization's STARMC and forensic activities.
- Establish communication and escalation channels between the STARMC, forensics team, UIDAI and the other ecosystem partners
- Propose Data and Evidence Management Procedures and Systems and the Legal, and Regulatory components that may need to be incorporated
- Develop security incident tracker and establish a process along with responsibilities to drive security incidents to logical closure
- Design dashboard for reporting and maintain knowledgebase of learnings from earlier security incidents
- The GRCP-SP shall ensure that the tools in the STARMC including Forensics Lab remain relevant to the emerging threats, updated and cost effective.
- Conducting scheduled and unscheduled preparedness drills including IT continuity drill
- Participation in preparedness drills organized by CERT-IN or any other third party appointed by UIDAI on a periodic basis

Deliverables

1. Design, Implement and obtain acceptance for fully functional STARMC including Forensics Lab as per above outlined requirements.
2. During the Operations Phase the bidder is required to Review and report on the STARMC design on an annual basis.
3. Scheduled and unscheduled drill reports to assess the preparedness of ecosystem partners – can include penetration testing, vulnerability assessment, ethical hacking (including but not limited to).
4. STARMC IT Continuity Drill Report on an annual basis

10.3.2. 24*7 - Continuous monitoring of CIDR, DC, DR, Perimeter Security and other key IT Infrastructure Facilities

Security issues are critical for the success of pervasive Aadhaar project. GRCP-SP would be responsible to manage a perimeter security for UIDAI infrastructure. GRCP-SP would be responsible to:

- Oversee the UIDAI infrastructure on an ongoing continuous basis and check if all ecosystem/ user touch points are adequately secured.
- Monitor the Multi-layer security employed by UIDAI ecosystem partners starting with networks, perimeter, demilitarized zone (DMZ), Data Center, applications and databases and wherever required, provide recommendations to improve safeguarding of UIDAI system.
- Continuously (24*7) identify all types of network attacks and recommend counter measures.
- Monitor whether a role based access control at all levels is being followed by the UIDAI ecosystem.
- Maintain extensive logs at all levels and associated tools for audit and quick alerting in case of unforeseen malicious access.
- Verify whether all the hardware assets are adequately secured throughout their life cycle as they may contain sensitive data

Objective

The objective of doing a 24*7 - Continuous monitoring of CIDR, DC, DR Infrastructure is to monitor and assess the conformance by the MSP (or other ecosystem partner as the case may be) and Data Center Service Provider and add value to improve the CIDR, DC, DR operations.

Overview of Scope

The MSP / ecosystem partner and data center providers are responsible for the proper functioning of CIDR and Data Centers. GRCP-SP would have oversight responsibility for 24*7 continuous monitoring of SOC and NOC managed by MSP / ecosystem partner. GRCP-SP will assess current capabilities for intrusion detection, traffic monitoring, and log aggregation/correlation as well as service performance monitoring arrangements. The GRCP-SP shall also be responsible for 24*7 continuous monitoring of security and privacy incidents and frauds.

GRCP-SP is required to establish a continuous monitoring strategy and implement a continuous monitoring program that includes:

- a. Ongoing security control assessments in accordance with UIDAI's continuous monitoring strategy with an overall objective of reducing/ minimizing security and privacy incidents and frauds
- b. An on-going determination of the security impact of changes made to UIDAI CIDR, DC and DR infrastructure.
- c. Reporting the security state of the information system to appropriate officials of UIDAI and/or UIDAI ecosystem

Key Activities

Continuously assess the security of the infrastructure and application components leveraging automated mechanisms. The key activities under 24*7 monitoring include:

- End to end correlation of states and events across all stakeholders of UIDAI as mentioned in coverage scope
- Maintaining a secure and centralized repository of all audit trails / logs generated by various systems (for duration of 7 years in a secure and encrypted manner as follows: **2 years on line and 5 years offline**)
- Logging, identifying root causes and managing all security and privacy incidents and frauds in a timely and workflow based mechanism (Security incidents shall include - incidents; suspected incidents; near-misses; suspected near-misses)
- Performance of specific desktops, users, groups, servers, disk utilization, services such as email and browser, software such as applications and database, network bandwidth usage, sessions and latency for the purpose of performance SLA's oversight
- Maintaining a comprehensive list of threat and countermeasures, vendor patches and vulnerabilities, effects of emergency policy changes, signature updates, outages
- VA and PT scanning of network and application assets daily and on-demand to identify, track, report and alert on system vulnerabilities (quarterly schedule and daily schedule for some identified critical devices, services, software)

- Black box and white box penetration testing of the network from outside and inside on regular frequency
- Blocking, warning and alerting in real time where actions are prohibited or need business justification, quickly identifying unauthorized access and activity
- Evidence handling and storage of data including volatile data during investigations, email tracing, disk imaging, recovery of deleted files / fragments of data / passwords, identifying phishing sites and their takedown, recreation of time critical events, network session analysis and extracting files from sessions, database forensics, collaborating with law enforcement for investigations, civil injunctions or search orders (For all incidents and frauds lifelong storage; fraud persons data can be sent to vigilance, etc.)
- Providing a single real time view for performance of the UIDAI ecosystem with drill down to the component level
- The GRCP-SP needs to do an Information Security Assessment as per ISO 27001 framework including Monitoring, Maintenance and Management of the entire CIDR, DC, DR, Perimeter Security and other key locations and provide recommendations to the UIDAI. GRCP-SP would be responsible for 24*7 continuous monitoring of SOC and NOC, CIDR, DC, DR and other key infrastructure installations.
- Monitor, identify and suggest corrective measures for aspects such as Missing patches / outdated software / Mis-configurations / Inadequate hardening / Presence of malware / rogue devices / Abuse of privileges / Use of dormant accounts and accounts with excessive privileges / Use of in-secure network services, communication protocols / Leakage of sensitive data / Perimeter Security

Deliverables *(inclusive but not limited to)*

5. Daily performance, alerts and monitoring reports
6. Deviation, deficiency, controls performance, controls coherence, VA and PT reports
7. Role based access, unauthorized access or usage reports
8. Asset inventory reports
9. Report and document misuse of data, applications and networks
10. Report on vulnerabilities by type or severity level, malicious code by type, remediation tasks by status
11. Detailed reports on suspected incidents; near-misses; suspected near-misses
12. Severity based incident and fraud logging and tracking report
13. Investigation progress report
14. Blocking, warning and alerting reports
15. Action plan and progress for the week report
16. Metrics based dashboards

Based on the above, the GRCP-SP shall prepare the following for each incidence of security incident/ fraud:

17. Incident Management Report
18. Incident Closure Report
19. Fraud Detection and Management Report
20. Fraud Closure Report

The above are list of Reports that GRCP-SP is required to design and implement as part of the operations phase on an ongoing basis.

*As part of the 24*7 operations GRCP service provider shall appropriately consider the following UIDAI requirements and incorporate the same in their technical proposal and deliverables.*

Infrastructure

- GRCP-SP shall deploy detectors and sensors or use data feeds from the existing detectors and sensors such as the following (Below list is indicative and not exhaustive)
Anomaly detection, anti-virus, data security, intrusion detection and prevention, malware and malware removal, messaging security, multifactor authentication, patch management, PC security, secure remote administration, security policy management, threat management, transaction monitoring, user authentication, web security, log management and analysis, configuration assessment / vulnerability detection
- Ensure and identify minimum bandwidth, performance overhead on existing infrastructure and additional storage requirements, transmission and retention of data in encrypted form
- Infrastructure for risk simulation, risk rating and analytics

People and skills

It is required that the GRCP Service Provider shall staff adequately for the activities for 24X7 security monitoring operations. It is expected that across the levels, the team brought in by GRCP-SP shall be of higher training and experience than that of a “classic” SOC / NOC operational team.

10.3.3. Periodic Assessments & Reviews

Security issues are critical for the success of pervasive Aadhaar project. GRCP-SP would be responsible to manage a perimeter security for UIDAI infrastructure. GRCP-SP would be responsible to:

- Oversee the UIDAI infrastructure on periodic basis and check if all ecosystem/ user touch points are adequately secured.
- Monitor the Multi-layer security employed by UIDAI ecosystem partners starting with networks, perimeter, demilitarized zone (DMZ), Data Center, applications and databases and wherever required, provide recommendations to improve safeguarding of UIDAI system.
- Identify all types of network attacks and recommend counter measures.
- Monitor whether a role based access control at all levels is being followed by the UIDAI ecosystem.
- Maintain extensive logs at all levels and associated tools for audit and quick alerting in case of unforeseen malicious access.
- Verify whether all the hardware assets are adequately secured throughout their life cycle as they may contain sensitive data

As part of UIDAI GRCP initiative to enhance oversight on the ecosystem processes and partners, there is an increased emphasis on the on-going reviews and assessments to ensure effective compliance to UIDAI IS policy and identified controls.

GRCP-SP shall carry out periodic assessments and reviews to provide an independent and objective opinion on whether adequate controls are in place to effectively manage the risk (including frauds) posed to UIDAI information assets. The GRCP-SP shall broadly adhere to below steps to carry out these reviews.

Assessment / Review Plan: The GRCP-SP shall prepare a *“plan and an approach”* to carry out IS and process fraud reviews and assessments to comprehensively cover various UIDAI processes and ecosystem partners and share the same with UIDAI for final approval. Here the focus will be on the effectiveness of the plan regarding the coverage of key **Information security/ privacy/ fraud risks** that are identified as relevant for UIDAI functioning. The same shall be submitted to UIDAI for final sign off. *It is of paramount importance that the plan and the approach are totally in line with the overall GRCP framework to enable seamless work distribution, reporting, escalation and issue resolution.*

Carry out Assessments / Reviews: GRCP-SP shall carry out the assessments and reviews as per the approved plan and periodicity. GRCP-SP shall work closely with UIDAI to ensure availability of key personnel, access to facilities and infrastructure while covering the UIDAI processes and ecosystem partners.

Reporting& Closure of findings: The GRCP-SP shall submit reports as per the agreed periodicity. The reporting shall follow the flow of submitting a Draft Report to UIDAI and discuss the findings. These findings are communicated to the respective process owners / ecosystem partners for resolution. Working along with UIDAI, process owners and ecosystem partners, the GRCP-SP shall play a primary role to ensure all identified issues are resolved / corrected within the pre-defined timelines. Once the identified issues are addressed, GRCP-SP shall submit the final report along with implementation plan and suggested measures for all unresolved issues.

As part of these periodic assessments GRCP-SP is required to cover all the ecosystem partners and their processes. GRCP-SP as part of these assessments outlined in the following sections is required to *perform on the ground assessment at the ecosystem partner's physical locations/ sites.*

Further, for carrying out these periodic assessments, the GRCP-SP is required to bring in and deploy appropriate Information technology and tools that will support effective and integrated assessment of all UIDAI ecosystem partners.

The GRCP-SP shall carry out these periodic assessments in a manner that will ensure equitable distribution of auditable entities and processes throughout the year so as to ensure availability of respective ecosystem partners/ owners for these reviews. The approach should also ensure optimal utilization of GRCP-SP resources and report preparation. The understanding of this approach should be adequately reflected in the proposed technical approach and methodology.

Periodic Assessment (inclusive but not limited to)		
S. No.	Type of Assessment	Periodicity
1	Application Security Assessment	Annual
2	Infrastructure Penetration testing	Half-Yearly
3	Security Focused Code Review	Annual
4	Security Centric SDLC Review	Annual
5	BCP / DR Process Assessments	Half-Yearly
6	Security review of changes to UIDAI ecosystem processes/technology solution / infrastructure	Need basis
7	Network Assessment: Local Area Network Infrastructure	Half-Yearly
8	Network Assessment: Wide Area Network	Half-Yearly
9	Physical Security Assessment – CIDR / DC / DR	Half-Yearly
10	Information Security Awareness/Social Engineering Review	Half-Yearly
11	Security Exception Management	Quarterly
12	Biometric Solutions related Assessments	Annual
13	Root Cause Analysis Assessments	Need basis
14	Security Assessment of Data Encryption and Key Management	Half-Yearly
15	Security Assessment of Portable Devices	Half-Yearly
16	Information security assessment of SDLC process	Annual
17	Validate the "Solution Acceptance Process"	Half-Yearly
18	Validate the "Infrastructure Acceptance Process"	Half-Yearly
19	Validate the "BoM Acceptance Process"	Half-Yearly
20	Review Biometric De-duplication process	Half-Yearly
21	Process Fraud Risk Assessment	Half-Yearly
22	Review and validate Fraud Management process	Half-Yearly
23	Review and validate secured letter printing and dispatch process	Half-Yearly
24	Reviews for SLA Process Assurance	Half-Yearly

10.3.3.1. Information Security Assessment (this review shall include specific requirements as outlined in UIDAI IS Policy)

Objective

The objective of Information Security Assessment is to ensure that the ecosystem partners are adhering to the IS policy, procedures and controls as defined by the UIDAI and assure the overall design and implementation effectiveness throughout all UIDAI processes and among all the ecosystem partners. This review shall check for the compliance of ecosystem partners against the information security policies and guidelines issued by the UIDAI and provide recommendations to the UIDAI so as to ensure confidentiality, integrity and availability of information and resources.

a. Information Security Assessment of Ecosystem Partners

As part of Periodic Assessments w.r.t. Information Security, Privacy and Continuity GRCP-SP is required to cover the following UIDAI ecosystem partners and their respective processes and infrastructure

External Ecosystem Partners	Internal Ecosystem Partners
Registrar	Managed Service Provider
Enrollment Agency	Biometric Service Provider
Testing and Certification Agency	Data Center Service Provider
Training Agencies	Logistics Service Provider
Authentication User Agencies	Contact Center
Authentication Service Agencies	ASDMSA

As part of these periodic assessments GRCP-SP is required to cover all the ecosystem partners and their processes. GRCP-SP as part of these assessments outlined in the following sections is required to **perform on the ground assessment at the UIDAI ecosystem partner's physical locations/ sites.**

It is required to cover 25% of the each of the external ecosystem partners on an annual basis, except for AUAs which shall be limited to 25 AUAs per year and cover 100 % of all internal ecosystem partners annually as part of Information Security Assessment.

Further, for carrying out these periodic assessments, the GRCP-SP is required to bring in and deploy appropriate Information technology and tools that will support effective and integrated assessment of all UIDAI ecosystem partners.

Deliverables for information security assessments as outlined in the subsequent sections shall adequately incorporate the findings/gaps and recommendations individually and w.r.t. each of the above UIDAI ecosystem partners

b. Application Security Assessment

GRCP-SP shall assess the security of the in-scope applications from the perspective of an unauthenticated user and authenticated users with varying level of privileges aimed at bypassing inter-user access control restrictions, escalating privileges at the application level, obtaining unauthorized access to sensitive data and gaining privileged access to the underlying infrastructure or data. The in-scope application to be assessed includes but is not limited to the following:

- Enrolment Client & Enrolment Server Application
- SFTP Client
- UIDAI Public Portal & Partner Portal
- AADHAAR Authentication Service
- Critical identified applications managed by MSP / ecosystem partner
- Aadhaar Payment Bridge and Aadhaar Enabled Payment System

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

21. Outputs / reports generated by the tools used for vulnerability scans
22. Description of identified application vulnerabilities and the implications of successful exploitation of the identified vulnerabilities
23. A composite risk rating for each of the identified vulnerabilities considering the business impact of successful exploitation, popularity of the vulnerability and simplicity of attack techniques
24. Examples of data extracted from the system in case the vulnerability could be successfully exploited during the penetration test
25. Recommendations to address the root cause of the identified vulnerabilities
26. List of affected menu options, URLs and parameters for each of the identified vulnerabilities
27. Integration of all open/work-in-progress/closed issues with Compliance / Executive Dashboard

c. Infrastructure Penetration testing

GRCP-SP shall assess the security of the UIDAI's infrastructure components with the objective of obtaining unauthorized access to sensitive data internally and externally, gaining privileged access to the targeted infrastructure and using a compromised target as a vantage point to further penetrate the CIDR landscape

- External penetration test from the perspective of an unauthenticated external attacker targeting the SFTP servers, terminals used by AUA, AUA Servers, infrastructure supporting public / partner portal, authentication services and critical identified network/systems in CIDR landscape reachable from internet
- Network devices and servers across the CIDR landscape including the Data Centre, development network at the Tech Centre, UIDAI HQ as well as regional offices
- Registrar / enrolment agency operators / Last Mile Logistics Services Provider targeting the SFTP servers and the infrastructure components in the DMZ
- Aadhaar Payment Bridge and Aadhaar Enabled Payment System

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

28. Outputs / reports generated by the tools used for port and vulnerability scans
29. Outcome of basic footprint checks such as ICMP scans and trace route
30. List of accessible TCP & UDP based services
31. Description of vulnerabilities affecting the network accessible services and the implications of successful exploitation of the identified vulnerabilities for each of the target hosts
32. A composite risk rating for each of the identified vulnerabilities considering the business impact of successful exploitation, popularity of the vulnerability and simplicity of attack techniques
33. Trophies demonstrating the extent of system compromise in case the vulnerability could be successfully exploited during the penetration test
34. Recommendations to address the root cause of the identified vulnerabilities
35. Integration of all open/work-in-progress/closed issues with Compliance / Executive Dashboard

d. Security Focused Code Review

GRCP-SP shall perform a static code analysis and manual review of the security aspects of the in-scope applications in order to identify security flaws and potentially malicious code embedded within the applications, including but not limited to,

- Enrolment Client

- SFTP Client
- Enrolment Server Application
- UIDAI Public Portal & Partner Portal
- UIDAI Authentication Client Library

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

36. Description of application vulnerabilities identified and the implications of a successful exploitation of the identified vulnerabilities
37. Prioritization of the identified vulnerabilities based on the risk perceived to the organization
38. Recommendations to address the root cause of the identified vulnerabilities
39. List of affected pages and parameters for each of the identified vulnerabilities
40. Integration of all open/work-in-progress/closed issues with Executive Risk Dashboard

e. Security Centric SDLC Review

GRCP-SP shall review the SDLC processes at UIDAI to determine the extent to which information security requirements are addressed during the various stages of SDLC

- Enrolment Client
- SFTP Client
- Enrolment Server Application
- UIDAI Public Portal & Partner Portal
- UIDAI Authentication Client Library
- Any ancillary application connecting to CIDR repository and/or related systems

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

41. Description of risks identified at each phase of the SDLC process
42. Design level gaps identified between the As-Is process and leading practice
43. Recommendations to address the gaps identified during the various stages of SDLC
44. Integration of all open/work-in-progress/closed issues with Executive Risk Dashboard

f. BCP / DR Assessments

GRCP-SP shall assess compliance of BCP / DR policies and adherence to BCP procedures spelt out for UIDAI. Review of compliance to BS25777 standard for:

- CIDR DC, DR Operations

Implementation Gap Analysis Report

45. Implementation gaps identified between the As-Is process and procedures spelt out in the IT DR for UIDAI
46. Integration of all open/work-in-progress/closed issues with Executive Risk Dashboard

g. Security review of changes to UIDAI ecosystem processes/technology solution / infrastructure

GRCP-SP shall, on a need basis, review and assess the overall security posture of the UIDAI ecosystem due to any changes made to UIDAI ecosystem processes, technology and critical ICT infrastructure. The review shall cover the below:

- All UIDAI Processes/Infrastructure
- All UIDAI Ecosystem Partner Interface processes/ Infrastructure
- All CIDR, Authentication and Enrollment Processes/ Infrastructure
- Aadhaar Payment Bridge and Aadhaar Enabled Payment System

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

47. Review feedback for changes submitted to UIDAI
48. Approval/Rejection recommendations as appropriate
49. Summary of approved/rejected changes on a monthly basis

h. Network Assessment: Local Area and Wide Areas Network Infrastructure (Different elements of network like Core, distribution, Access, DMZ, MZ, Regional offices, Data Center, Security devices)

- Validate the implementation of the UIDAI Local Area and Wide Area Network with respect to the requirements as per the overall UIDAI technology solution and security Architecture requirements
 - UIDAI LAN
 - MPLS UIDAI Network
 - Point to Point DC connectivity
 - Internet Connectivity at CIDR, Regional Data Center and Authentication Data Centers.
 - Partner Management System
 - Network Security systems
- Verify the Network Functional Compliance

- Review the High Level and Low level Design Documents
- Review requirement traceability matrix
- Assess and review the deployment practices of network deployment across multiple zones w.r.t industry practices
- Regular review of vendor product and software releases prioritization of implementation of new releases /changes and analyze the impacts on UIDAI network.
- Review Network Operating System qualification / deployment / configuration process.

Findings and Recommendation Report

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

50. Functional Compliance Report – Detailing the compliance – non-compliance of the Network w.r.t the requirement in the RFP for each subsystem/module in the CIDR Network (DMZ, MZ, Management Network, Backup Network, Regional offices, Regional Data Centers, Authentication Data Centers, etc.)
51. Report the vendor software and hardware releases and vulnerabilities and Prioritization in line with CIDR network and also the Gap Report.
52. Detailed Analysis Report of the RCA - including classification of root causes, remedial measures for preventing the same in future.
53. Vulnerabilities analysis in MZ, DMZ, Network Security devices, Management Network and Backup Network, Regional office network, Regional Data Center and Authentication infrastructure network. The report should provide the Vulnerabilities, rating, and gaps with recommendation
54. Review of change management – planned and unplanned changes and approvals reporting

i. Physical Security Assessment – CIDR / DC / DR

Perform Physical Security Assessment for UIDAI ecosystem facilities including CIDR, DC, DR, Registrar Premises which house Infrastructure related to UIDAI processes, Enrolment Agencies, Secure Letter Printing Facilities, Software Development Facilities, and Call Center. GRCP- SP shall evaluate physical security controls and environmental controls. Key areas that GRCP-SP should assess as part of Physical Security Assessment include the following:

- Physical Access Control to Buildings: Facility Security - Entry points, Data center, User and sensitive environments, Access control and monitoring devices, Guard personnel, Wiring closets
- Internal Company Personnel - Control and accountability, Use of equipment, Security procedure compliance, Awareness, Use of break areas and entry points
- External Visitor and Contractor Personnel - Control and accountability, Use of equipment, Security procedure compliance, Use of break areas and entry points

- Physical Access Control to Information Technology Resources: Computer Systems and Equipment – Workstations, Servers, Backup media, PDAs, Modems and other physical access points
- Sensitive Information and Data – Control, Storage, Destruction
- Physical Security Control Mechanisms within the Server or Critical processing areas.
- Business Continuity Plan.

Findings and Recommendation Report

55. Detailed Physical Security Assessment Technical Report – Facility Wise. Next-step recommendations

j. Information Security Awareness/Social Engineering Review

The objective of social engineering review is to test the effectiveness of the UIDAI's IS policies as well as security awareness among UIDAI employees and its ecosystem partners.

- GRCP-SP shall assess the effectiveness of training and awareness to UIDAI employees and its ecosystem partners on social engineering attacks and phishing schemes which can divulge confidential information.
- Assess information security awareness levels for the UIDAI staff and identified individuals in the UIDAI ecosystem
- Social engineering audits and assessments for randomly selected staff across levels
- GRCP-SP shall consider social engineering attacks and phishing schemes such as Spear Phishing, Media Mailing, Onsite Media Drop, Phone Pretexting (IT/Help Desk and End Users), Onsite Pretexting, Client Public Information Profiling, etc.

Findings and Recommendation Report

56. Information Security Awareness/Social Engineering Review Report and recommendations.

k. Personnel Security

Identify and report information security exceptions w.r.t personnel security against UIDAI security policies within UIDAI ecosystem. The GRCP-SP shall review and report on the following at a minimum.

- Review, assess and report on the process of documenting Security roles and responsibilities as part of job definitions where appropriate
- Review, assess and report on the process of conducting Verification checks on permanent staff at the time of job application and selection

- Confidentiality or non-disclosure agreements to be signed by employees are part of their terms and conditions of employment. Contract or third party users to sign a confidentiality agreement prior to being given system access.
- Review, assess and report on the Terms and conditions of employment and the employees responsibility for information security
- Review and assess the process of the training and updates provided to employees (and relevant third parties) on information security
- Review, assess and report on the process, knowledge and awareness of Security incident reporting

Findings and Recommendation Report

57. Information Security Review and Assessment Report (w.r.t. UIDAI ecosystem personnel) and recommendations.

1. Security Exception Management

GRCP-SP shall establish a security exception management process. During the operations phase GRCP-SP is required to identify and report information security exceptions against UIDAI security policies within UIDAI ecosystem (especially CIDR, enrollment and authentication processes). The Security Exception Management reporting shall cover the below:

- All UIDAI internal processes/infrastructure
- All UIDAI Ecosystem Partner Interface Processes/ infrastructure
- All CIDR, authentication and enrollment processes/ infrastructure
- Aadhaar Payment Bridge and Aadhaar Enabled Payment System

Findings and Recommendation Report

58. Finalize the Security Exception Management Process

59. Security exception dashboard for tracking exception review and closure on a monthly basis

60. Risk mitigation controls to indirectly remediate security issues

61. Integration of all open/work-in-progress/closed issues with Executive / Compliance Risk Dashboard

10.3.3.2. Biometric Solutions related Assessments

One of the critical resources that can be misused are the facilitation centers that help in recovering lost UIDs, change enrolled images (of poor quality), etc. security procedures at such points should be carefully assessed.

Assessment of Processes related to Biometric

- Review and audit of the enrollment process, including biometric data capture, demographic data entry, enrollment operator authentication, local de-duplication, encryption and key management, and maintenance/upgrade of the enrollment hardware/software.
- Review and audit of the CIDR middleware and UID generation. This includes isolation of PII from BSP, Encryption changes and key management, verification of identities of enrollment station, agent and registrar.
- Review and audit of the manual verification process
- Review and audit of the certification process of devices and adherence to conditions of quality of data (appropriately for enrollment and authentication), and availability of drivers for all platforms mentioned.

Security consideration related to Biometric Solution that shall be covered as part of this assessment shall include the below:

- Template/Data protection in CIDR (de-duplication).
- Template/Data protection in Authentication servers including transaction records Encryption of data in enrollment records during transit
- Physical and process security of CIDR in terms of data access.
- Review of data dissemination portals (both public and to registrars) to ensure PII is not leaked.
- Review of the effectiveness of disincentives to avoid duplicate enrollments and imposter authentication, other than through technical means.

Findings and Recommendation Report

62. Biometric Solutions Related Assessment Report – This report shall cover the Detailed Information Security Assessment and Exception Report and recommendations w.r.t. Biometric Solutions covering the above requirements.

10.3.3.3. Root Cause Analysis Assessments

There may be instances when UIDAI technology solution is exposed to events which lead to failure of services of UIDAI such as high/critical incidents or defacing of UIDAI website or advanced persistent threats or UIDAI infrastructure/application sabotage. UIDAI shall initiate an ‘On Demand’ audit as and when UIDAI services are compromised.

The following is an indicative list of events which may cause services of UIDAI to be disrupted or compromised and trigger a Root Cause Analysis Assessment:

- Unavailability of Enrolment Service
- Unavailability of Authentication Service
- Unavailability of Applications, Portals, EMS, BMS etc.

- Denial of Service Attack
- SQL Injection Attack
- Issuance of duplicate-ids
- Loss of enrolment data
- Failure due to a disaster
- Failure in disaster recovery and business continuity plan

GRCP-SP shall perform Root Cause Analysis for suspect events as well and report on the same.

Overview of Scope

The above assessments shall be ‘on-demand’ and shall be triggered by UIDAI on need basis.

- GRCP-SP shall on a short notice mobilize the team for on-demand assessments.
- GRCP-SP shall identify the components affected/ compromised/ failed and its dependency and impact on other components.
- GRCP-SP shall identify the root cause for the failure or disruption in service, clearing highlighting all the possible causes and their impact.
- GRCP-SP shall do an impact assessment of the event quantifying the loss to the UIDAI.

Key Deliverables

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

63. GRCP-SP shall submit a **Detailed Impact Assessment Report** on the events/suspected events or risks which lead to disruption in services of UIDAI. The report shall include root cause analysis, components effected, impact assessment recommendations for prevention and remedial, implementation plan for remedial measures. The report may also attempt to calculate and quantify the loss to UIDAI due to the event.

10.3.3.4. Security Assessment of Data Encryption and Key Management

Objectives

UIDAI collects a vast amount of personal data of Indian residents with the help of a large number of enrolment agencies spread all over India. With the advent of Aadhaar enabled payment system and Aadhaar Payment Bridge, a lot of registrars, PDS's and financial institutions are poised to employ Aadhaar based authentication for their service disbursement. These transactions shall happen over a broad spectrum of networks and devices. Hence, it becomes highly important for carrying out secure transactions to prevent

misuse of data. The information security policy states that all the data transfers to and from UIDAI to its entire ecosystem partners have to be encrypted. Thus, GRCP-SP has to do the important task of assessing the actual implementation of encryption standards and key management, to safeguard the information security related to UIDAI business transactions and the privacy of Aadhaar users.

Overview of Scope

GRCP-SP shall carry out security assessments of end-to-end encryption from the point of encryption to the point of decryption. This should encompass complete Point-Of-Transaction installation, integration, network assessment, application testing, inbound and outbound transaction testing, device assessment, encryption evaluation, forensic analysis and field testing.

The assessment should test across administrative, technical and physical controls. Wherever control gaps/vulnerabilities are identified, remediation guidance should be communicated and follow-up testing should be performed to validate gap closure. It will also be responsible to assess and monitor if key management i.e. procedures and protocols used for key generation, transfer and all other key handling mechanisms are robust and effective enough to prevent failure. GRCP-SP should also suggest best practices in data encryption and key management to UIDAI.

Data Encryption

Based on the data protection risk assessment, for encrypting confidential, and other agency-sensitive data the GRCP-SP shall review, provide policy recommendations and facilitate implementation of identified controls with respect to Data Encryption Technologies and processes implemented in UIDAI ecosystem.

- GRCP-SP shall review and report on the compliance level of encryption mechanisms implemented to comply with UIDAI IS policy
- Review if the confidentiality of data at rest on computer systems owned by and located within UIDAI ecosystem and networks is maintained and ensure whether it is protected by either Encryption, or Firewalls with access controls that authenticate the identity of those individuals accessing the specific systems/data or other compensating controls including complex passwords, physical isolation/access.
- Review and report on hard drives that are not fully encrypted, e.g., have encrypted partitions, virtual disks, etc.
- Encryption of Back up / stored data security (e.g., file systems, disks, heterogeneous tape drives, virtual tape libraries) in a (e.g., Storage Area Network/ Direct-Attached Storage/ Network-Attached Storage) environment.

- Key length requirements to be reviewed on a periodic basis and recommend upgrades as technology allows.
- Review and report the use of proprietary encryption algorithms.

Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. GRCP-SP shall review the Key management procedures and provide recommendations and facilitate implementation as a primary responsibility to ensure that only authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements.

- Generation processes for different cryptographic systems and different applications
- Distribution, access, and activation for authorized users
- Storage, Archiving, and Destruction
- Changes and updates, including rules on when keys should be changed and how this will be done;
- Compromises or loss of control incidents
- Revocation with specific withdrawal or deactivation procedures
- Recovery when lost or corrupted as part of business continuity planning

Deliverables *(inclusive but not limited to)*

- 64. Security Assessment report of data encryption
- 65. Security Assessment report of key management

10.3.3.5. Security Assessment of Portable Devices

Specific and highly stringent monitoring controls to be designed implemented and reported to restrict unauthorized exposure and distribution of confidential and sensitive data

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential and sensitive data are the result of stolen or lost Portable Computing Devices.

The best way to prevent these exposures is to avoid storing confidential data on these devices. As per the UIDAI IS policy, confidential or sensitive data should not to be copied to or stored on a portable computing device or a non-UIDAI owned computing device without written authorizations from two signatories at a minimum.

As part of the review process, GRCP-SP at a minimum shall verify the following.

- Written authorizations as per UIDAI IS Policy, that verify a legitimate business need for accessing and storing confidential /sensitive information on a portable device
- All users obtaining specific permission from the data owner before storing confidential or sensitive data on a portable computing device.
- Protection mechanisms on Portable devices & Removable Media containing Confidential or sensitive information
- Secure Storage of Portable devices & Removable Media containing Confidential or sensitive information
- Secure Packing and Transportation of Portable devices & Removable Media containing Confidential or sensitive information
- Process of Dispatch and Receipt of Portable devices & Removable Media containing Confidential or sensitive information
- Inventory Report on Portable devices & Removable Media containing Confidential or sensitive information

Deliverables

66. Portable devices & Removable Media Security Assessment report / Findings (including violations) and Recommendation Report capturing the above aspects

10.3.3.6. Information security assessment of software development, testing facilities and review and validation of SDLC process (SW Development, Release Management, Version Control, etc.)

Objective

The process of software development for UIDAI system adopted by the ecosystem partners should adhere to the accepted standards and best practices. While these standards are to be proposed by the ecosystem partners, the GRCP-SP is expected to review them to ensure that the standards adopted are in compliance with the UIDAI IS policy.

Overview of Scope

The GRCP-SP is expected to verify the compliance to agreed upon SDLC process from time to time. The GRCP-SP will verify and validate that all key aspects of application software development like version control, coding standards, test plan and methodology, release management and related policies are documented and are being followed by the ecosystem partners.

Key Activities

- During the **Initiation Phase**, the GRCP-SP should conduct risk assessments and validate the definitions regarding the high-level information security policy requirements.
- During the **Development/Acquisition Phase**, the software development ecosystem partners will define the system's security and functional requirements. The GRCP-SP should verify the test cases for UAT and Functional Compliance Test prepared by the MSP / ecosystem partner for security compliance.
- During the **Implementation Phase**,
 - GRCP-SP should verify the design reviews and system tests performed by MSP / ecosystem partner, before placing the system into operation to ensure that it meets required security specifications. GRCP-SP should check for the following security tests carried out: check and test applications for Denial of Service, Phishing Attacks, Spoofing, Replay Attacks, Substitution attack, Tampering, Masquerade attack, Trojan Horse Attacks, Overriding Yes/No response, Aggregate Attacks
 - Based on this, it has to give final acceptance to the newly developed software or suggest security improvements ("solution acceptance process")
 - GRCP-SP should assist UIDAI in updating the security certifications after implementing new software
- During the **Operations Phase**, the GRCP-SP should continuously monitor performance of the newly developed system to ensure that it is consistent with the UIDAI IS policy
- During the **Disposal Phase**, GRCP-SP should oversee the information preservation, media sanitization and Hardware/Software disposal processes to ensure that the confidentiality, integrity and availability of data is in accordance with UIDAI IS policy
- If any deviations are identified in any of these stages, then the GRCP-SP should escalate the same to the UIDAI and the MSP / ecosystem partner, along with suggestions on the corrective measures to be undertaken.
- GRCP-SP should also test the accuracy and usability of the SLA monitoring tools deployed by the MSP / ecosystem partner to verify whether the tools deployed provide an accurate, correct, measurable and verifiable estimation of the system performance, as per the Service Level Requirements listed in the MSP RFP.
- GRCP-SP should validate the vulnerability assessment testing, penetration assessment testing etc. conducted by MSP / ecosystem partner

Deliverables *(inclusive but not limited to)*

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

- 67. Threat analysis report
- 68. Functional Compliance Report
- 69. Test Coverage Report
- 70. Detailed Risk Analysis report of SDLC process management

10.3.3.7. Validate the "Solution Acceptance Process", "Infrastructure Acceptance Process" and "BoM Acceptance"**Objective**

The objective of performing a validation of the "Solution Acceptance Process", "Infrastructure Acceptance Process" and "BoM Acceptance" is to ensure that the system specifications and functional specifications, acceptance plan, production scenarios and test cases that have been shared by various ecosystem partners comply with UIDAI security policy and requirements.

Overview of Scope

Validation of "Solution Acceptance Process", "Infrastructure Acceptance Process" and "BoM Acceptance" for all the ecosystem partners is to be performed annually and the relevant changes in the year of the audit shall be recorded. The base asset register with necessary details shall be provided by UIDAI.

Deliverables *(inclusive but not limited to)*

List of Reports that GRCP-SP is required to design and implement as part of the operations phase (inclusive but not limited to)

- 71. Asset inventory reports
- 72. Functional Compliance Report
- 73. Technologies assessment report
- 74. Solution / BoM / Infrastructure Acceptance report

10.3.3.8. Review of Demographic and Biometric De- duplication process

Objective

UIDAI visualizes issuing unique Aadhaar number to all the residents in India, to eliminate repeated KYC checks by service providers and prevention of leakage in government social expenditure through de-duplication of beneficiary lists and establishing identity of beneficiaries. Hence, to meet these objectives and maintain uniqueness, Biometric and Demographic de-duplications are very important processes during generation and issuing of Aadhaar numbers. The GRCP-SP vendor is required to review and validate the entire de-duplication process from an accuracy and performance point of view

Overview of Scope

Demographic de-duplication is used primarily to catch trivial duplicates (non-fraudulent cases where all the demographic fields are identical) that are inadvertently submitted to the system e.g. repeat enrolment or when a resident has not received Aadhaar number in a few days and decides to re-enroll, verification for children under the age of 5 year as biometrics is not captured . The UIDAI uses both exact-match and fuzzy-match strategies to improve the demographic de-duplication accuracy.

For Biometric de-duplication, UIDAI technology solution makes use of multi-modal de-duplication using an in build **Automated Biometric Identification Subsystem (ABIS)**. The demographic and biometric data of residents captured by the enrolment agencies are sent to the CIDR. Multiple modalities i.e. fingerprint and Iris are used for de-duplication. This is routed through Multi-vendor multi-modal solutions to carry out the distributed computing of de-duplication. The **UID Biometric middleware** is used to provide vendor independence and standardization.

In the event of duplicate enrolments, the ABIS will pass back a ReferenceID and the scaled comparison scores upon which the finding was based.

Key Activities

- Measuring of accuracy and reliability of the multi-modal biometric data captured at enrolment centers so as to prevent false matches
- Detailed study of the types of biometric methods being used so as to validate the standards in which duplicates are identified
- Review the effectiveness of strategies used in demographic de-duplication
- Evaluating if the speed and accuracy of matching is adequate

- Review of the algorithms/software and hardware infrastructure used for de-duplication
- Review of network infrastructure between the servers, middleware and the array of multi-modal solutions of different vendors (routing and mediation, Guaranteed delivery, Fault tolerance and load balancing)
- Review of the Anonymity procedures enforced on data before going to the ABISs
- Review of Integrity, confidentiality, privacy and encryption of data transfers between the UID servers and ABISs
- Cost effectiveness of de-duplication efforts
- Reviewing the manual adjudication process and standards for adjudicating duplicate cases

Deliverables

75. Detailed Compliance Report for Demographic and Biometric De-duplication process

10.3.3.9. Fraud Risk Management

The GRCP-SP shall design and institutionalize a Fraud Risk Management (FRM) process to identify and address the Fraud Risk within the processes of UIDAI and its ecosystem partners. The GRCP-SP is required to design a Fraud Risk Management process that will include characteristics such as following:

“Deterrence” to design and institutionalize controls and accountabilities with an intention to discourage a fraud before it is attempted or prevent a fraud from occurring.

“Detection & Mitigation”, design and institutionalize processes to detect and locate fraud and mitigate the impacts/ losses.

“Analysis & Investigation”, identify and analyze the suspect / fraudulent activities to determine the factors and control lapses, root cause analysis, etc. Obtain evidence either to stop an ongoing fraudulent activity, recover associated losses, and to support successful prosecution of the individuals involved in fraudulent activities.

GRCP-SP is required to bring in and deploy appropriate Information technology and tools that will support effective and overall Fraud Risk Management within UIDAI and its ecosystem partners. However, as part of the FRM design considerations, GRCP-SP shall ensure a tight integration and optimal use of the infrastructure, tools and facilities that are set-up in the STARMC including Forensics Lab and the Fraud Risk Management platform brought in by MSP / ecosystem partners.

As part of the Fraud Risk Management function and ongoing review GRCP-SP shall assess associated risks and report on the following:

- Current and future anticipated avenues for fraud attempts entering the UIDAI system (internal and external)
- Avenues for misuse of enrolment, updation and authentication
- Process and policy for preventing, monitoring and handling attempted frauds
- Implications and de-risking approaches for UIDAI to consider, in scenarios where frauds are successful in penetrating the UIDAI system

The risks identified from above fraud reviews shall be incorporated and reported as part of the overall Risk Assessment Report.

The design of overall governance structure should incorporate formal roles for effective Fraud Risk Management.

*The Fraud Risk Management function shall be run as a seamless and single process which tightly integrates the inputs and intelligence from both 24*7 continuous monitoring activities and fraud management process.*

Deliverables:

76. Design of Fraud Risk Management Policies, Procedures, Roles and Responsibilities
77. Implementation of Tools as required for effective FRM (should be implemented as part of STARMC (including Forensics Lab))
78. Fraud scenario/ pattern report for UIDAI and its ecosystem partner processes, esp. for enrolment, updation and authentication on an annual basis
79. Fraud Risk Analysis and Management Reports
80. Fraud Detection and Management Report – to be developed for each individual pattern/ event
81. Fraud Closure Report - to be provided for each individual pattern/ event

10.3.3.10. Review and validate Fraud Management process

Objective

To prevent problems of duplicate or ghost beneficiaries from seeping into the Aadhaar database, the UIDAI proposes to have a fraud monitoring mechanism to prevent misuse (including exception handling mechanism) by any ecosystem members.

The objective of reviewing and validating the Fraud Management process is to detect and reduce identity fraud. GRCP-SP has to periodically review and validate this Fraud management processes for their effectiveness in preventing the perpetuation of frauds into the CIDR.

Overview of Scope

GRCP-SP would be responsible to review and validate fraud management system adopted by MSP / ecosystem partner and other ecosystem partners and assess the detection, prevention mechanisms which are being done by rule-based, prediction-based techniques and subsequently inspected manually.

Key Activities

- As part of governance structure, GRCP-SP would ensure that an adequate fraud risk management program is in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.
- Fraud risk exposure should be assessed periodically by the GRCP-SP to identify potential schemes and events that the UIDAI needs to mitigate.
- GRCP-SP should review and validate the effectiveness of prevention techniques to avoid potential key fraud risk events and ways to mitigate possible impacts.
- GRCP-SP should review and validate the effectiveness of Detection techniques to uncover fraud events when preventive measures fail or unmitigated risks are realized.
- GRCP-SP should review the investigation and corrective action methods used for addressing potential fraud in an appropriately and timely manner
- GRCP-SP should recommend based on leading practices in fraud management.

Deliverables *(inclusive but not limited to)*

82. Assessment report of Fraud management system

83. Recommendation report for Fraud management mechanisms

10.3.3.11. Review and validate secured letter printing and dispatch process

Objective

GRCP-SP is required to review the entire logistics process and validate its effectiveness in maintaining the required security and confidentiality of inbound and outbound data. GRCP would be responsible to oversee whether the processes followed for data transmission from

enrolment agencies/ecosystem partner to CIDR and from CIDR to ecosystem partner /Department of Post (DoP) and delivery of printed UID letter to the Resident is adhering to UIDAI IS policy or not.

Overview of Scope

The core logistics activities: printing, sorting, dispatching and delivery of the Aadhaar letter is currently handled by Department of Posts. The Managed Service Provider (MSP) or any agency appointed by UIDAI shall primarily be responsible for managing and monitoring the logistics provider as a part of logistics services functions by using a Logistics Interface application.

GRCP-SP shall be responsible to monitor whether the MSP / ecosystem partner and other Logistics Service Providers are adhering to the security policy as stated in the UIDAI IS policy guidelines and that the letter printing and dispatch process is secured. GRCP-SP should ensure that the data transmitted through Logistics Interface Application is adhering to the UIDAI IS policy for delivery of enrolment packets from enrolment agencies to CIDR and delivery of printed UID letter to the Resident.

Key Activities

- Reviewing whether the MSP / ecosystem partner and logistics provider are adhering to the UIDAI IS security policy
- Reviewing and validating the security of data transfer done by MSP / ecosystem partner and DoP as part of the Logistics processes as mentioned below:
 - Uploading of enrollment data from regional offices to CIDR network
 - Tracking the delivery of enrolment packets from enrolment agencies to CIDR
 - Check for completeness and correctness of content received
 - Sending UID data for letter printing and delivery
 - Receiving daily status updates on the inbound and outbound sides
 - Sealing, encoding and dispatching memory stick as per UIDAI guidelines to CIDR.
 - Sending electronic batch file of enrolments to CIDR.
 - Tracking the delivery of printed UID letter to the Resident
- Review and validate the IT infrastructure and network equipment for inbound and outbound logistics with respect to UIDAI IS Policy
- Review the deviation reporting process followed by the MSP / ecosystem partner with respect to UIDAI IS Policy

Deliverables *(inclusive but not limited to)*

84. Security assessment report of Logistics process and system

10.4. Performance

10.4.1. Reviews for SLA Process Assurance and SLA measurement on a sample basis

Objective

GRCP-SP shall provide SLA process assurance through periodic oversight and SLA measurement on a sample basis so as to enable ecosystem partners to achieve higher service levels.

Overview of Scope

The GRCP-SP is required to review the SLA measurement process being followed by respective ecosystem partners to monitor and report their promised SLAs and validate the effectiveness of measurement method.

The GRCP-SP should review, validate and document, the performance of ecosystem partners as per the criteria set by UIDAI. It should test and report the robustness of the SLA measurement processes against the Performance SLAs as defined for ecosystem partners. The GRCP-SP shall also perform actual SLA measurement on a sample basis (5%) as per the defined SLA measurement process and record findings as part of the report.

Key Activities

- Review and validate the SLAs defined for various ecosystem partners to review and monitor the performance with reference to the SLA
- Provide assurance for data centre, applications, biometric solutions, authentication, logistics, contact centre and enrollment agency metrics such as resource utilization, false reject rate, de-duplication rate, letter printing turnaround time, complaint resolution time, successful biometric enrollments, etc. from a performance SLA process oversight perspective
- Provide assurance regarding performance of specific desktops, users, groups, servers, disk utilization, services such as email and browser, software such as applications and database, network bandwidth usage, sessions and latency for the purpose of performance SLA's process oversight
- Tabulate, in a template, all possible measurable parameters as defined in the SLA. The performance of these parameters shall be checked on a sample basis (5%) to compare and assess the actual outcomes. The results shall be collate and reported to the UIDAI

- Review the SLA performance on a quarterly basis and suggest improvements for the same

Deliverables *(inclusive but not limited to)*

List of Reports that GRCP-SP is required to design and implement (as part of the operations phase) with minimum coverage (inclusive but not limited to)

85. SLA measurement framework

86. Service maturity index

87. SLA performance reports (covering the below items at the minimum)

- Sample SLA measurement report
- Deviation and deficiency reports
- Action plan and progress for the week report

As part of the SLA Process measurement activity, GRCP service provider shall appropriately consider the following UIDAI requirements and incorporate the same in their technical proposal and deliverables

Infrastructure

- GRCP-SP shall deploy/use data feeds from the existing detectors and sensors deployed by the UIDAI ecosystem partners.
- Ensure and identify minimum bandwidth, performance overhead on existing infrastructure and additional storage requirements.

10.5. Technology refresh**Objective**

Considering the long term nature of GRCP operations and based on the risk analysis, risk simulations of threat and frauds, various global trends analysis (threats, risks, frauds), technology advancements analysis applicable to UIDAI, etc. carried out by the GRCP-SP, it is required that the GRCP-SP shall provide a detailed technology refresh plan which should bring in the thought leadership point of views on how it proposes to address this with the goal that UIDAI is always protected and continues on a path of operational efficiency maturity.

(As part of the technical proposal, the bidder shall also provide a detailed technical write up to address the technology refresh component that is in line with the overall UIDAI goal to always remain protected and continues to be on a path of operational efficiency maturity.)

Overview of Scope

- GRCP-SP shall be responsible for the following activities as part of technology refresh.
 - a. Forecasting requirements of STARMC including Forensic Lab for technology refresh
 - b. Track key technology trends, threats, risks etc. and determine key technology refresh areas
 - c. Identify potential alternative technologies and solutions that can be deployed in STARMC and Forensics Lab and develop analysis parameters in consultation with UIDAI
 - d. Prepare and submit a technology refresh plan to UIDAI Board/ Technology Architecture Review Board (TARB) for appropriate actions. This plan shall comprise of:
 - Drivers for technology refresh
 - Key options and evaluation of each option
 - Costs associated, if any, with the technology refresh
 - Plan for implementation of technology refresh
 - Likely impact, if any, on service level agreements of UIDAI ecosystem partners
 - Expected cost reduction, if any, due to induction of new technology
 - Expected process and SLA improvements of UIDAI ecosystem partners
- The triggers for technology refresh shall be one or more of the following:
 - Change in Risk and Threat Landscape
 - Technology advancements
 - Improvement opportunities for Incident related metrics
 - Improvement opportunities in Security maturity and performance of service
 - Opportunity for return on security investment
 - Total Cost of Ownership (TCO)

Deliverables (inclusive but not limited to)

1. Technology Refresh Plan including Thought Leadership views on an annual basis.

Please note that the Technology Refresh Plan is forward looking input. The GRCP-SP in its current technical and commercial proposal is expected to factor in the required infrastructure and processes to meet the SLAs and Scope of Work as defined in this RFP.

10.6. Exit / Transition Management

Objective

The objective of this section is to define generic guidelines about transition methodology from the GRCP-SP for effective management of the transition of responsibilities. The purpose of transition is to ensure seamless continuation of operations and knowledge transfer.

Overview of scope

Exit Management Plan: GRCP-SP shall provide a recommended Exit Management Plan. The exit management plan will be reviewed by UIDAI and if required may be suitably modified by the GRCP-SP to cover all aspects during the transition period and upon acceptance by the UIDAI, will be implemented by the GRCP-SP.

Transfer of Assets: GRCP-SP shall transfer both IT and non IT Assets acquired for the GRCP project to UIDAI. The list of assets shall cover those under the purview of current GRCP-SP including Consortium Partners.

Transfer of Agreements: GRCP-SP shall arrange or provide support for Assignment / Transfer / Novation of Agreements with all the OEMs who are being used by the current GRCP-SP in the execution of the GRCP project.

Provision of Information: GRCP-SP shall provide access to information reasonably required to define the current mode of operation associated with the provision of services and also access and copies of all information / data / documentation/ files/ procedures/ configurations/drawings/ records, prepared or maintained, pertaining to GRCP (including 24*7 security monitoring operations, forensics and fraud, performance assessments), services rendered including but not limited to applications, Business and IT Operations, and other performance data. GRCP-SP shall not purge or destroy any copies of documents and records related to services being rendered for UIDAI.

Access Rights: GRCP-SP shall provide reasonable rights of access to prospective Service Provider to GRCP Project Locations and premises where assets are located. Provide access to prospective Service Provider /UIDAI employees and facilities as reasonably required to understand the methods of delivery of the services employed by the prospective Service Provider and to assist appropriate knowledge transfer.

Personnel: GRCP-SP shall provide a list of all employees (with job titles) of the Current GRCP-SP dedicated to providing the services. To the extent that any Transfer Regulation

does not apply to any employee of the current GRCP-SP, the current GRCP-SP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by UIDAI or the prospective Service Provider in case an offer of employment or contract for services is made to such employee.

Knowledge Transfer: In this phase, GRCP-SP should assemble the core team for knowledge transfer. This team will then take the team of prospective Service Provider through classroom sessions, demonstrations and study of critical applications and their alignment to the UIDAI services. IT infrastructure of the vendor (servers, network diagrams, monitoring equipment, and databases) and various processes shall be explained by current GRCP-SP team to reasonable satisfaction to UIDAI/prospective service provider.

Following are the guidelines for GRCP-SP to carry out transition:

- i. The GRCP-SP shall carry out transition as per provisions of the contract between GRCP-SP and UIDAI.
- ii. GRCP-SP shall allow the UIDAI authorized vendor/agency/prospective Service Provider to conduct due diligence activities prior to the transition.
- iii. GRCP-SP shall assist the prospective Service Provider formulate transition plan, assess the resource requirements and form a transition team for knowledge acquisition
- iv. GRCP-SP shall assist the prospective Service Provider in defining the success parameters for the transition
- v. GRCP-SP shall assist the prospective Service Provider obtain a detailed understanding of current operations and associated SLAs.
- vi. GRCP-SP shall share the knowledge bank consisting of all the process documentation, technology documentation and services management documents.
- vii. GRCP-SP shall conduct a thorough walkthrough for the prospective Service Provider about the activities done by the GRCP-SP and clarify any queries that may be posed by the prospective Service Provider
- viii. GRCP-SP shall assist UIDAI in assessment of the level of knowledge acquisition by the team of prospective Service Provider
- ix. A phase of assisted operations shall be provided by the GRCP-SP during which the prospective Service Provider shall carry out the entire portfolio of GRCP-SP operations under supervision of GRCP-SP.
- x. As part of the selection/bid process for the prospective Service Provider, GRCP-SP, in presence of UIDAI, shall provide and assist with knowledge sharing sessions/ walkthroughs/ site visits, such that it equips various bidders with sufficient knowledge to prepare and submit their respective bids. Any questions that the bidders may have towards the scope of work shall be answered in detail by GRCP-SP. In case certain documents are to be shared with prospective bidders, GRCP-SP shall provide the same upon receiving a written request from UIDAI.

Deliverables (inclusive but not limited to)

1. Exit Management Plan (covering the below items at the minimum)
 - Training Materials
 - List of Assets (IT and non IT) which are to be transferred to UIDAI
 - List of Employees worked on the project

10.7. Summary of list of deliverables (indicative but not limited to)

S.No	Section	Sub Section	D. No.	Deliverable	Periodicity	Deliverable Applicability	
						Design and Implementation Phase	Operations Phase
1	Governance	GRCP Governance Framework	a	GRCP Vision Document	One Time for design.	Y	
			b	GRCP Framework and Program Design	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			c	Initial Risk Assessment/GAP Report	One Time for design.	Y	
			d	Updated version of Baseline Information Security Policy for GRCP ecosystem	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			e	Strategic Analysis Report	One time as part of Design and Implementation Phase; Review on an Half Yearly basis subsequently	Y	Y
		GRCP Organization, skills and people	f	Finalized GRCP Organization Structure	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y

			g	Finalized Job Definitions and Specifications	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			h	Finalized Roles, Profiles and User Assignment	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			i	Performance Measures for all KEY profiles	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
		GRCP Communication, Reporting & Decision Making	j	Finalized Communications Plan & System Requirements	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			k	Finalized Reporting Standards including the mechanisms, formats and automation requirements	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			l	Finalized Executive Support System incorporating Executive & Compliance Dashboards	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			m	Finalize and Implement Escalation	One time as part of Design and Implementation Phase; Review on an Annual basis	Y	Y

				Procedures	subsequently		
			n	Incident related metricsreport	Quarterly		Y
			o	Resilience trends and metricsreport	Quarterly		Y
			p	Regulatory compliance progress	Annual		Y
			q	GRCP benchmark metrics	Annual		Y
			r	Security maturity and performance of service reports	Annual		Y
			s	Process maturity metrics and maturity index reports	Annual		Y
2	Risk	Risk Assessment, Prioritization & Treatment	a	Information Risk Assessment report of the UIDAI ecosystem	One time as part of Design and Implementation Phase; Review on an Quarterly basis subsequently	Y	Y
			b	Risk analysis scope document for ecosystem partners	Annual		Y
			c	Risk Register, Risk & Controls Matrix	Quarterly		Y
			d	Develop Risk Treatment Plan which includes Risk Mitigation Plan and	One time as part of Design and Implementation Phase; Review on an Quarterly basis subsequently	Y	Y

				Acceptance Criteria.			
			e	Unified risk index view	Quarterly		Y
			f	Controls effectiveness, efficiency and maturity report	Annual/ Need Basis		Y
		Risk Profiling	g	Risk Profiles – Process / Function Wise / Eco System Partner Wise	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			h	“White-list” of applications and infrastructure – Process / Eco System Partner Wise	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			i	Report on risks to availability, confidentiality, and integrity of information	One time as part of Design and Implementation Phase; Review on an Quarterly basis subsequently	Y	Y
		Risk Intelligence	j	Design and Implement a Global risk intelligence feed dashboard	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			k	Expected future threats and risk mitigation plan reports	Half-Yearly		Y

			l	Threat exposure and forecast report	Half-Yearly		Y
			m	Pattern analysis report	Half-Yearly		Y
			n	Trend report of category wise threats	Half-Yearly		Y
			o	Benchmark report against organizations in India and globally	Annual		Y
			p	Report on threats by technology, severity, type and impact to UIDAI	Half-Yearly		Y
			q	Weakest link reports for return on security investment	Half-Yearly		Y
			r	Consistency reports for return on security investment	Half-Yearly		Y
			s	Efficiency reports for return on security investment	Half-Yearly		Y
			t	Opportunity report for return on security investment	Half-Yearly		Y
3	Compliance-Ongoing	Design and Set up of STARMC	a	Design, Implement and obtain acceptance for fully functional STARMC including Forensics	One Time	Y	



RFP for the Selection of the GRCP-SP

				Lab			
			b	Review and report on the STARMC design	Annual		Y
			c	Drill reports	Half-Yearly / Need Basis		Y
		24*7 - Continuous monitoring	d	Performance, alerts and monitoring reports	Ongoing		Y
			e	Deviation, deficiency, controls performance, controls coherence, VA and PT reports	Ongoing		Y
			f	Role based access, unauthorized access or usage reports	Ongoing		Y
			g	Asset inventory reports	Ongoing		Y
			h	Report and document misuse of data, applications and networks	Ongoing		Y
			i	Report on vulnerabilities by type or severity level, malicious code by type, remediation tasks by status	Ongoing		Y

			j	Detailed reports on suspected incidents; near-misses; suspected near-misses	Ongoing		Y
			k	Severity based incident and fraud logging and tracking report	Ongoing		Y
			l	Investigation progress report	Ongoing		Y
			m	Blocking, warning and alerting reports	Ongoing		Y
			n	Action plan and progress for the week report	Ongoing		Y
			o	Metrics based dashboards	Ongoing		Y
		Incident Management	p	Incident Management Report	Ongoing		Y
			q	Incident Closure Report	Ongoing		Y
			r	Fraud Detection and Management Report	Ongoing		Y
			s	Fraud Closure Report	Ongoing		Y
4	Compliance-Periodic Assessments & Reviews	Information Security Assessment	a	Application Security Assessment-Findings and Recommendation	Annual		Y

				Report			
			b	Infrastructure Penetration testing- Findings and Recommendation Report	Half-Yearly		Y
			c	Security Focused Code Review- Findings and Recommendation Report	Annual		Y
			d	Security Centric SDLC Review- Findings and Recommendation Report	Annual		Y
			e	BCP / DR Process Assessments- Implementation Gap Analysis Report	Half-Yearly		Y
			f	Security review of changes to UIDAI ecosystem- Findings and Recommendation Report	Need Basis		Y
			g	Network Assessment- Findings and	Half-Yearly		Y



RFP for the Selection of the GRCP-SP

				Recommendation Report			
			h	Network Assessment-Functional Compliance Report	Half-Yearly		Y
			i	Network Assessment-Detailed Analysis report of the RCA	Half-Yearly		Y
			j	Network Assessment-Vulnerabilities analysis report	Half-Yearly		Y
			k	Network Assessment- Review of change management	Half-Yearly		Y
			l	Physical Security Assessment- Physical Security Assessment Technical Report	Half-Yearly		Y
			m	Physical Security Assessment-Next-step recommendations	Half-Yearly		Y
			n	Information Security Awareness/Social Engineering Review Report and recommendations	Half-Yearly		Y



RFP for the Selection of the GRCP-SP

			o	Personnel Security Report and recommendations	Half-Yearly		Y
			p	Security Exception Management-Findings and Recommendation Report	Quarterly		Y
		Biometric Solutions related Assessments	q	Biometric Solutions related Assessments	Annual		Y
		Root Cause Analysis Assessments	r	Detailed Impact Assessment Report	Need Basis		Y
		Assessment of Data Encryption and Key Management	s	Security Assessment report of data encryption	Half-Yearly		Y
			t	Security Assessment report of key management	Half-Yearly		Y
		Security Assessment of Portable Devices	u	Findings and Recommendation Report	Half-Yearly		Y
		SDLC process security assessment	v	Threat analysis report	Annual		Y
			w	Functional Compliance Report	Annual		Y

			x	Test Coverage Report	Annual		Y
			y	Detailed Analysis report of the RCA	Annual		Y
		Validation of "Solution Acceptance Process", "Infrastructure Acceptance Process" and "BoM Acceptance"	z	Asset inventory reports	Half-Yearly		Y
			aa	Functional Compliance Report	Half-Yearly		Y
			ab	Technologies assessment report	Half-Yearly		Y
			ac	Solution / BoM / Infrastructure Acceptance report	Half-Yearly		Y
		Review of Biometric De-duplication process	ad	Detailed Compliance Report for Biometric De-duplication process	Half-Yearly		Y
		Fraud Risk Management	ae	Design of Fraud Risk Management Policies, Procedures, Roles and Responsibilities	One time as part of Design and Implementation Phase; Review on an Half Yearly basis subsequently	Y	Y
			af	Implementation of Tools as required for effective FRM	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			ag	Fraud scenario/ pattern report for UIDAI and its ecosystem partner	Half-Yearly		Y



RFP for the Selection of the GRCP-SP

				processes			
			ah	Fraud Risk Analysis and Management Reports	Half-Yearly		Y
			ai	Fraud Detection and Management Report	Need Basis		Y
			aj	Fraud Closure Report	Need Basis		Y
		Review and validate Fraud Management process	ak	Assessment report of Fraud management system	Half-Yearly		Y
			al	Recommendation report for Fraud management mechanisms	Half-Yearly		Y
		Review and validate secured letter printing and dispatch process	am	Security assessment report of Logistics system	Half-Yearly		Y
5	Performance	Reviews for SLA Process Assurance	a	SLA measurement framework	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y
			b	Service maturity index	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y



RFP for the Selection of the GRCP-SP

			c	SLA performance reports	Quarterly		Y
6	Technology Refresh		a	Technology Refresh Plan	Yearly		Y
7	Exit Management		a	Exit Management Plan	One time as part of Design and Implementation Phase; Review on an Annual basis subsequently	Y	Y

10.8. Roles and Responsibilities of UIDAI:

As the owner of the Project for “Design and implementation of the GRC Framework and providing Performance Assurance Services” the role of UIDAI in the successful implementation includes discharging the following responsibilities:

- i. The UIDAI shall appoint an officer – in – charge of Information Security and Privacy (at a DDG level) for overseeing and being responsible for Information Security and Privacy at UIDAI. GRCP-SP shall report into this officer-in-charge.
- ii. The UIDAI shall be responsible to appoint a nodal officer for monitoring and coordinating the implementation of the GRCP project and to liaison with UIDAI board/ TARB for issuing necessary instructions, approvals, commissioning, demonstration of applicability of utilization, Acceptance certificates, Go-live, rewards, penalties and payments etc. to the GRCP-SP.
- iii. The UIDAI shall ensure that timely approval is provided to the GRCP-SP as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfillment of this contract. The UIDAI shall approve all such documents within 15 business days.
- iv. The UIDAI's representative shall interface with the GRCP-SP, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. UIDAI shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the UIDAI is proper and necessary.
- v. UIDAI may provide on GRCP-SP's request, particulars/information/ or documentation that may be required by the GRCP-SP for proper planning and execution of work and for providing services covered under GRCP project and for which the GRCP-SP may have to coordinate with respective vendors.
- vi. UIDAI shall review and approve the solution design, implementation approach, and other reports as submitted by the GRCP-SP. As per the approved GRCP framework and implementation plan, UIDAI shall ensure all tools and technologies required for effective GRCP functioning shall be implemented/deployed/integrated as the case may be on to the UIDAI ecosystem partner's infrastructure.
- vii. UIDAI shall identify ecosystem partners and ensure their availability in terms of their time, personnel and access to the facilities for carrying out periodic GRCP audits and assessments.
- viii. UIDAI shall provide necessary support during requirement gathering, sharing of sample reports and other IT infrastructure requirements to GRCP-SP. In case of incident/fraud, UIDAI shall facilitate interactions with the law enforcement agencies, media and appropriate Government agencies.

- ix. UIDAI shall provide appropriate authority and powers to GRCP-SP for performing its role and scope as outlined in this section. ***GRCP-SP would be provided with appropriate decision making power on behalf of UIDAI to safeguard UIDAI interests in case of critical incidents.*** This authority and power shall be communicated in writing by UIDAI Board/ TARB so as to enable GRCP-SP to respond to and facilitate closure of various incidents/fraud.
- x. UIDAI shall identify and provide to the GRCP-SP within four weeks of contract signing, site and space (primary and secondary locations) to establish the STARMC including Forensics Lab.
- xi. UIDAI shall identify and deploy adequate number of personnel on a 24*7 basis in the STARMC.

11. Implementation Schedule

This section outlines the proposed key delivery timelines and the implementation schedule for the GRCP-SP.

S. No.	Activity/Task/Milestone	Timeline (in weeks)
Design and Implementation Phase		
1	Team mobilization and commencement of work	T* +4 weeks
2	Detailed Project Plan	T + 7 weeks
3	GRCP Vision, Strategy, Framework and Programme Design	T + 14 weeks
4	Finalize Risk Assessment and Risk Profiling Methodologies	T + 16 weeks
5	Design and Institutionalize Risk Intelligence Capability	T + 20 weeks
6	Risk Assessment Report/ Gap Report	T + 16 weeks
7	Risk Treatment Plan	T + 20 weeks
8	New UIDAI IS Policy Documentation	T + 18 weeks
9	Baseline Risk Profiles for ecosystem processes and partners	T + 20 weeks
10	Finalization of GRCP Organization, Roles, Profiles and User Assignment	T + 20 weeks
11	Communication, Reporting & Decision Making (Communications Plan, Reporting Standards, Executive Support System, Compliance Dashboards, Escalation Procedures etc.)	T + 20 weeks
12	Finalize the plan for Periodic Assessments and Reviews	T + 18 weeks
13	Finalize the plan for SLA Process Assurance and Measurement	T + 18 weeks
14	Date of Site handover by UIDAI to GRCP-SP for setting up of STARMC including Forensics Lab	SHO**
15	Supply, Procurement and Commissioning of Hardware for STARMC including Forensics Lab (after handing over of site by UIDAI)	SHO + 12 weeks
16	Supply and Implementation of Software for STARMC including Forensics Lab	SHO + 16 weeks
17	Supply and Implementation of GRCP tools	SHO + 16 weeks
18	Acceptance and Go-Live	SHO + 20 weeks



RFP for the Selection of the GRCP-SP

Ongoing Operations Phase		
19	Operations - Beta Phase (STARMC, Forensics Lab, Periodic Assessments, SLA Process Assurance, Risk Intelligence)	SHO + 24 weeks
20	Operations - Steady State (STARMC, Forensics Lab, Periodic Assessments, SLA Process Assurance, Risk Intelligence)	SHO + 24 weeks and 24*7 thereafter

*T - Date of Signing of Contract

** SHO – SHO is defined as the date of Site handover by UIDAI to GRCP-SP for setting up of STARMC including Forensics Lab, which should be taken as 4 weeks from the date of signing of contract.



12. Bill of Material

Sl No.	Tool Category	Indicative Tool Description	Capacity Required	Data to be maintained	Retention Time	Primary	DR	Offered License Description	
						Server Quantity*		per Unit Cost	Enterprise License Cost
1	Analysis / Correlation of Security Logs, Network Traffic and	Audit Trail/Log Management	All UIDAI devices across 2 Primary Data Centres and 8 Regional Data Centres , totaling over 20,000 devices; 100,000 EPS	Audit Trails and reports	2 years online and 5 years offline				
2	Network Behavior Anomaly	Network Traffic Analytics	All UIDAI egress points across 2 Primary Data Centres and 8 regional Data Centres , totaling 2*1GBPs links	Traffic Data	3 months				
3		Network Behavior Anomaly	All UIDAI egress points across 2 Primary Data Centres and 8 regional Data Centres , totaling 2*1GBPs links	Reports	7 years				
4	Network Security Analytics & Replay	Session and Attack replay and analysis	Enterprise scale	Reports and sessions	7 years				
5	Malware Analysis	Sandbox for malware analysis on premise	Covering analysis and simulation of all malware identified and captured that are targeted at UIDAI	All results and reports	7 years				



RFP for the Selection of the GRCP-SP

6		Analysis utilizing global intelligence	Global Threat Intelligence feeds and platform to share threat information with relevant authorities		Real time				
7	Forensics and Fraud analysis	Network Forensics Tool	All UIDAI egress points across 2 Primary Data Centres and 8 regional Data Centres , totaling 2*1GBPs links	All Test results and closure reports	7 years				
		Host Forensics Tool	All servers and desktops within UIDAI	All Test results and closure reports	7 years				
8	Risk Simulation	Risk modeling and simulation	Enterprise scale	Reports and models	3 months				
9	GRC	Incident and Compliance Management	All security incidents and investigations, from start to closure, covering people, process and ICT	All Data associated with the processes identified	7 years				
10		Audit Management	All internal, external, self-audits performed by GRCP team and information about all audits performed by MSP to be maintained						
11		Risk Management	All risk identified by GRCP team and associated process data						
		Vulnerability and Penetration Testing	All UIDAI ICT devices across 2 PDCs and 8 RDCs						



RFP for the Selection of the GRCP-SP

		Application Security Testing	All UIDAI applications						
12		Performance Management	All performance parameters and process within GRCP scope						
13		Any other Governance Process e.g. security awareness program, ISO 27001 control management etc. proposed by GRCP solution provider	All other activities performed by GRCP vendor						
14		SOC Dashboard and work area	Wall mounted panels for display of SOC dashboard, Workstations for 24*7 operations Any other ICT equipment required		7 years				
15		Any additional detector/sensor proposed as per the solution proposal	As per solution requirements		As per solution				

* If virtual servers are being offered, please mention the total number of virtual servers being considered. Please provide a separate table detailing the virtual server configuration and total physical infrastructure proposed to host the virtual systems.

General Tools/Data specification

1. All Tools proposed should be available in HA mode at Primary site if it is to be used for real time processing
2. All tools proposed should have hot failover capability to Disaster recovery site
3. All data collected and maintained by GRCP vendor should be available online at Primary site and backed up at Disaster recovery site. It should be possible to restore the data into to the available infrastructure provisioned at the DR site.
4. All tools proposed should be configured/customized as per UIDAI requirements and as proposed in the solution proposal.
5. All tools proposed should be possible to be configured/customized in future as per mutual agreement between UIDAI and GRCP solution provider
6. All software/OS/Hypervisor/hardware/storage/backup etc. and additional ICT devices required to perform the log and network security analytics, malware analysis, fraud and forensics analysis and other GRCP monitoring tools shall be included as part of financial quote. Technical specifications of such hardware/software/OS/Hypervisor/storage/backup etc. shall be detailed out for each such component.
7. UIDAI may provide the underlying network and rack space/power/data centre services for all equipment proposed. Required Rackspace, power, cooling and network requirements are to be specified as part of the overall proposal and provide your cost for the same in case UIDAI only provides a physical room. Kindly mention the room size that you may require. The location is expected to be next to / close to the UIDAI Data Centres in Bengaluru and New Delhi.
8. All solution requirements to provide for the indicated retention time is to be provided by the solution provider

12.1. Log, Network Analysis

Sl No	Requirement	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	The solution should provide capability to collect, store and search on full payload packet captures of network traffic and audit trail data from the existing NOC / SOC / SIEM solution at UIDAI or directly from end devices. The solution should allow analysis of the collected network traffic and audit trails in unlimited dimensions for complete situational awareness.		
2	The solution should provide the ability to view full captured network data or logs in near real-time as the Data Collection nodes capture the network data packets and audit trails		
3	The solution should have the ability to view trends within the captured data as well as provide the ability to replay the captured network data packets in a secure sandbox fashion		
4	The solution should be capable of: Capturing packets from an Ethernet link of at least 1 Gigabit per second (1 Gbps / 1000 Mbps) bandwidth; should also support 10G interface Minimally, support for Copper gigabit Ethernet, with the option for Fiber gigabit Ethernet; Analyzing IPv4 and IPv6 traffic		
5	The solution should support the ability to import from and export to industry-standard network capture file formats. Examples: pcap, Sun snoop, MS Network Monitor captures, Network Associate Sniffer/Sniffer Pro.		



RFP for the Selection of the GRCP-SP

6	The solution should allow search on more than just IP header information on captured packets. Examples: Search for domain names in HTTP traffic, Email addresses in SMTP traffic, etc. Provide screen shot samples on this capability. Describe in detail the product's searching capability and what it supports, i.e., binary, Unicode, common file types, text-based, regex, specific fingerprint data – hex, hash (MD5, SHA1, etc.), and describe any performance impact.		
7	The solution should provide visualization of the captured data flows and conversations.		
8	The solution should provide the ability to centrally manage the packet collection nodes distributed across various UID datacentres which are located at diverse geographic locations and segregated network zones protected by boundary control devices (firewalls, application proxy).		
9	The central management UI provided should be intuitive and user-friendly – provide / attach screenshots		
10	The solution should have the ability to identify hosts/endpoints by IP addresses, MAC addresses, names (DNS or NetBIOS), or other unique characteristics identified by the analyst. It should also support 802.1q VLAN tagging.		
11	The solution should have the ability to efficiently access, read, search, and process stored captured network packets that are in the multi-GB (100+) to possibly terabyte range and spans up to one year in duration.		
12	The solution should be able to filter as well as truncate network sessions. Example of the 2 parameters are as following » Filter - Advertisements (ends in “doubleclick.net”) - Software Updates (ends in “liveupdate.symantec.com”) - Media (ends in “player.xmradio.com”) - IP address (192.168.1.54...etc.) - Filter *(All), Keep email = scott4323@hotmail.com » Truncate		



RFP for the Selection of the GRCP-SP

	- Drop packet payload for port SSH and SSL		
13	The solution should take up no more than 5% of available network bandwidth between the individual Data Collection nodes and the Central Management appliance/software.		
14	The solution should have the ability to throttle the amount of data being sent from the Data Collection nodes to the Central Management appliance/software to control and limit the network bandwidth use, if necessary		
15	The solution should have the ability to integrate with any Standard Security Event and Incident Management (SEIM) product and pull audit trail information from the same. Provide a description of this capability and the integration approach.		
16	The UI provided should support drill-down capability from a high-level event down to the actual data flow and with full payload in a near real time manner. The drill down should support the ability to group viewing of the captured data by IP addresses, IP subnets, geographic locations, functional areas (i.e., business lines), Data Collection nodes (name, IP address, etc.), or other analyst selectable criteria.		
17	The solution should provide the ability to produce reports on enterprise wide statistics. For example, common trends for the day, week, month, year; aggregated events from multiple Data Collection nodes; policies in effect; custom groupings (IP addresses, IP subnets, DNS domains, names, functional areas, geographic locations, Data Collection nodes, etc.).		
18	The solution should provide flexible, WYSIWYG drag-and-drop report builder and scheduling engine for out-of-box as well as user-defined template, and ad hoc (custom) reports.		
19	The solution should have the ability to create canned, user-defined template, and ad hoc (custom) reports.		
20	Ability to export the internally generated reports to common file formats. Examples: XML, HTML, PDF, XLS, CSV, PPT, DOCX. Provide a listing of the supported file types.		



RFP for the Selection of the GRCP-SP

21	All communication between various components of the solution should be encrypted (mention encryption details)		
22	Must describe, in full detail, the system health and performance monitoring and alerting capabilities of the product, both the central management server and the data collection nodes		
23	Specifically for the Central Management appliance/software, the solution should support the ability to connect to industry standard SAN solution to store the captured network data. List the supported SAN interfaces (Fiber Channel, iSCSI, FCoE, iFCP, etc.).		
24	Comprehensive security logging and auditing capability, which captures (but not limited to) login, logout, configuration changes (what, when, who), policy changes (what, when, who), and updates (what, when, who)		
25	Must provide documentation describing, in technical details, the security protection and controls implemented by the product (central management server/application and the data collection node). Examples: access control, authentication, host-hardening, encryption, auditing		
26	Must provide technical documentation describing the network communication processes and flows between all components in the solution. Example: central management server communication with data collection nodes		
27	The solution should provide a common dashboard for analytics of both log and packet data to reduce the analytics time. Ex- clicking on an asset should be able to pull both network and log data for the asset		
28	The solution should provide the ability to export the assign hashes (sha-1 at least) to the collected data to ensure digital chain of custody.		

12.2. Network security analytics

Sl No	Requirement	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	The solution should provide capability for free-form contextual analysis using OSI Layer 2-7 Content captured in the traffic using a port and protocol agnostic manner over large amounts of data stored and analyzed within a big data environment.		
2	The solution should have ability to parse protocols like HTTP, FTP, TFTP, TELNET, SMTP, POP3, NNTP, DNS, HTTPS, SSL, SSH, Vcard, PG, SMIME, DHCP, NETBIOS, SMB/CIFS, SNMP, NFS, RIP, MSRPC, LotusNotes®, TDS(MSSQL), TNS(Oracle®), IRC, Lotus, MSNIM, RTP, Gnutella, YahooMessenger, AIM, SIP, H.323 etc. Net2Phone®, Yahoo Chat, SCCP (Cisco®Skinny), Bioorren, GTALK, Hotmail, Yahoo Mail, GMail, TOR etc.		
3	The solution should provide ability to write parsers for custom protocols		
4	<p>The analytical capability of the solution should include but not limited to</p> <ul style="list-style-type: none"> · Write and run custom traffic protocol parsers. Provide details and screen shot samples on this capability. · Run signature-based patterns based on traffic after it has been parsed. · Ability to “white-list” traffic from search results (size of list important) as well as search traffic for “blacklisted” hosts or domains (size of list important) <ul style="list-style-type: none"> • Use inbuilt GeoIP database • Use external threat databases(both open and commercial) • Use external tools like Google Maps to visualize network 		



RFP for the Selection of the GRCP-SP

	<p>traffic flow</p> <ul style="list-style-type: none"> · Ability to automatically extract certain files from packet captures and export to another system for analysis (example: send exes to a file server for antivirus scanning or perform malware analytics by static analysis of file) 		
5	Should provide 24x7 intelligence service that provides immediate access to multi-source threat-intelligence and reputational content for the solution infrastructure		
6	The solution should create comprehensive metadata in any combination from a network of any size, and should have the capability to be reported on, alerted, plotted over time and presented in interactive formats.		
7	The solution should be able to use the network traffic captured and reconstructed by the solution to provide a up-to-the-minute glimpse into incidents, threats, anomalies, misconfigurations, compliance violations, and other activities on the network.		
8	The solution should provide analytical capability that enables a user (e.g. an analyst, incident responder, investigator) to zoom in and out of collected traffic and to drill down and see exactly what transpired over the course of time.		
9	The solution should provide ability to efficiently scan through large volumes of objects such as audio, documents, images and video captured by the solution, render a visual timeline of an event, deeply interrogate all the activity (e.g. communications, data sent and received, audio transmissions, etc.), and understand all the rich context associated with each object.		
10	This visualization capability should enable users to leverage all the rules, keyword searches, and other filters created in analysis bench to further refine and process the presented information.		
11	The solution should provide the ability to create user-defined alerts.		
12	The solution should have the capability to ingest audit trail traffic collected by the SIEM solution and provide a unified interface to the analyst for audit and traffic trail analysis or alternately directly ingest the audit trail from the end devices.		



RFP for the Selection of the GRCP-SP

13	Should provide API/SDK for programmatic access to the capture infrastructure, which supports C, C#, Java, Python, Perl and Ruby.		
14	The system should centralize threat data from trusted sources in a searchable, standards-compliant database.		
15	The system's database requires no specialized administration skills.		
16	Threat definition should be flexible and include: Vulnerabilities Malicious code Geopolitical threats Patches		
17	The system should be pre-integrated with security intelligence feeds (e.g., iDEFENSE, Symantec DeepSight, iSIGHT Partners IntelliSIGHT, etc.)		
18	The system should have the capability to be populated with threat data from email advisories.		
19	The system should consolidate the results of multiple network scans and links those results directly to physical assets.		
20	The system should relate threats to the assets they affect, enabling the prioritization of patches or workarounds based on asset criticality.		
21	The system should present the crypto information involved in the encrypted session as presented in the ip packet		
22	The solution should provide the ability to parse applications like chats, voip, images, documents, executable, command line sessions, queries, emails etc.		
23	The dashboard should allow intuitive zoom in/zoom out with on demand session information on each image		
24	RBAC,HTML and PDF report formats should be included		
25	FIPS compliant SSL communications between components (please mention level)		
26	SDK should be available to use metadata in internal applications if required. The SDK should have full featured C, C#. Java, PERL, Python, and Ruby API that allows for read only access to query, search, and render local and remote data		

12.3. Malware Analysis

Sl No	Requirement	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	The solution should inspect all network sessions, regardless of protocol, for suspicious activity or files and detect and flag both suspicious network activity and files		
2	For each piece of executable content found on the network, the solution should provide automatic capability to <ul style="list-style-type: none"> Identify and capture of all executable and metadata from the network sessions that are captured real time and analyzed for malicious behavior across all protocols and ports Mimic the techniques of leading malware analysts by asking thousands of questions about a file and all of its related network behavior, without requiring a signature or a known “bad” action. Leverages threat intelligence by fusing and triangulating information from leading threat intelligence and reputation services to assess, score, and prioritize risks 		
3	The solution should provide Risk-based scoring methodology with all context behind a score exposed to help prioritize remediation efforts		
4	The solution should provide facility for anonymous submission of files to the security community for analysis, including white list/black lists, reputation services, dynamic/static analysis services and others		
5	Should provide for both on-premise and cloud based sandbox technology where the objectionable content may be executed and		



RFP for the Selection of the GRCP-SP

	inspected		
6	The system should integrate with external service providers like Virustotal, URLVoid, Bit9, robtex etc. to validate the indicators of malicious activity		
7	The system should allow specifying the in-house Antivirus to list of threats that were missed by deployed Antivirus.		
8	The system should perform static analysis of the submitted file(online/offline) by doing checks like - Files found to be XOR encoded, Files found embedded within non EXE formats (e.g., PE file found embedded in a GIF format), Files linking to higher risk import libraries , Files highly deviating from the PE Format, compare file size vs PE Size, Shifted PE Header inside the DOS Header etc.		
9	The solution should take into context the session information like source IP, country, domain name, organization, file name, directory used, port etc. to list indicators of malware		

12.4. Forensics

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	The solution should allow users to quickly and efficiently scan through large volumes of objects such as audio, documents, images and video captured by Analysis/Correlation tool, render a visual timeline of an event, deeply interrogate all the activity (e.g. communications, data sent and received, audio transmissions, etc.), and understand all the rich context associated with each object.		
2	The solution should allow finding all relevant information for an asset, user etc. including log files, network data, content, files etc.		
3	The solution should allow filtering data based on normalized data like event types, protocols, IP addresses, ports, content type, applications, browsers, attachments, crypto, mac address, file types, mac address, hostnames, country, domains, service types usernames, workstation names, logon types etc.		
4	The solution should allow saving the relevant data including logs, packets etc. with hashes etc. to maintain digital chain of custody		
5	The solution should allow extracting executable. Images, documents etc.		
6	The solution should allow analyzing the content through the malware analytics solutions automatically or in offline mode if required.		
7	The tool should allow importing external feeds from other systems like vulnerability data, asset criticality information from feeds like CSV files		

Note: Bidders are required to propose High End Forensic Workstation / Forensic Workstation and Forensics Kit to effectively deliver the above functionality. Technical specifications of High End Forensic Workstation / Forensic Workstation and Forensics Kit shall be detailed out for each such component.

Following additional Forensics Software with minimum technical specifications as given below should also be proposed and deployed:

12.4.1. Live Server Acquisition Software

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	Should allow examiner to take RAM dump from 32 Bit and 64 Bit Systems.		
2	Should allow examiner to capture System protected files like registry files		
3	Should extract information related to Currently logged on user / user accounts		
4	Should extract information of Installed applications and drives including network drives		
5	Should extract information of USB devices used in suspected machine		
6	Should support acquisition of suspected server RAID irrespective of Configuration		
7	Should provide Acquisition in Linux/windows/MAC disk format		
8	Should support making forensic image from a computer or laptop without opening its hard drive		
9	Should include USB External Storage of TWO Terabytes for creating forensic images and RAM Dumps		
10	Data transfer Speed of 3GB per minute		

12.4.2. Integrated Disk Forensics Software

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	Should have built in module to Create forensic images of suspected storage device in DD,EO1 format with authentication with MD5 and SHA1 or SHA 256 hash		
2	Should have built it module to extract and analyze vital information like typed web address, USB device information, saved passwords, OS install date, OS name and version etc.		
3	Should have built in module to Recover passwords (Password recovery Tool) from all popular (commercial and freeware) applications such as: <ul style="list-style-type: none"> • MS Office up to version 2010 • Adobe PDF • Win Zip, 7ZIP • Open Office Documents (Bidder shall provide the list of all such applications. Please refer the specifications on Password Recovery Toolkit given below.)		
4	Should allow examiner to perform distributed password recovery by harness idle CPUs across the network to decrypt files and perform robust dictionary attacks		
5	Should have Known File Filter hash library with minimum 45 million hashes		
6	Analyst should never lose work due to a crash, as components should be compartmentalized in database, worker and GUI		
7	Should allow user to create physical drive from image		
8	Should use robust database in background to store large amount of		



RFP for the Selection of the GRCP-SP

	data		
9	User should be able to Cancel/Pause/Resume processing		
10	Should show real-time processing status		
11	Should perform analysis of RAM dump and show all running processes including those hidden by rootkits		
12	Should support email analysis of various email clients like Notes NSF, Outlook PST/OST, Exchange EDB, Outlook Express DBX, Eudora, Thunderbird, Netscape, RFC 833		
13	Should Supports analysis of encrypted images with popular encryption technologies, such as Credant, SafeBoot, Utimaco, EFS, PGP and Guardian Edge with known passwords		
14	Should Create detailed reports and output them into native format, HTML, PDF, XML, RTF, and more - with links back to the original evidence		
15	Should support Apple/Mac based disk formats and file systems		

12.4.3. Password Recovery Toolkit bundle

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	Should come with a minimum storage of 9 terabyte to store rainbow tables		
2	Should break 40 bit password (file and login password) in few minutes		
3	Should come with software to import password protected files		
4	Should support password breaking of multiple files simultaneously		
5	Should have security dongle to prevent unauthorized access		
6	Should be compatible with Password Recovery Toolkit and Distributed Network Attack		

12.4.4. Steganography Investigation Tool

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	Should be capable of detecting Steganography Applications and files on computers		
2	Should be capable of detecting Steganography files on web page		
3	Should Detect suspicious files through blind anomaly-based approach		
4	Should have State-of-the-art image analysis with advanced image filters		
5	Should scan audio files, JPG, BMP, GIF, PNG etc.		
6	Should have State-of-the-art audio analyzer		
7	Should perform Rapid identification of over 500 known steganography program		

**12.4.5. Forensic disk duplicator –**

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	A HDD imaging hardware tool capable of copying drives at up to 9 GB per minute		
2	Built in SHA256		
3	Image to 2 drives simultaneously		
4	Wipe up to 3 Forensic Disk Duplicator drives simultaneously.		
5	Store entire images in single ISO (dd type files) file for ease of investigation.		

Email database analyzer, Malware identification system, and Portable forensic kit for on call incident management, Device for forensics extraction of data from SIM/Cell phone and GPS devices should also be proposed and deployed. Technical specifications shall be detailed out for each such component.



12.5. GRC

S. No.	Requirement	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	<p>UID is looking a flexible platform which will allow to centrally consolidate , automate , track and manage</p> <ul style="list-style-type: none"> - Corporate level Audits, Risks , Fraud incidents management - Branch level Audits, Risks , Fraud incidents management - Compliance Management - Risk, KRI, KGI, KPI and Controls Monitoring - Business Continuity Management - IT Security , Risk and Incident Management <p>of various disparate GRC processes.</p>		
	General Features		
2	<p>GRC solution should include out of the box, best practice based solutions which can be used as required by UID and will support following GRC Processes:</p> <ul style="list-style-type: none"> - Audit Management - COSO ERM based Risk Management - Fraud and other Incident Management - BS25777 based IT Continuity Management - Asset and Enterprise Hierarchy Management - Compliance Management - Policy Management - Threat Management - Vendor Management 		
3	Product should provide on-premise and hosted deployment models for the solutions		
4	Every Audit / assessment process (Audit, Risk, Incidents, and ITCM) should have Issue Management support comprising of workflow based "Findings / NCs Management, Remediation Plan Management, Deviation Management Support.		



RFP for the Selection of the GRCP-SP

5	System should provide UID to automate additional GRC processes as required by providing framework to create new applications or changing existing ones using GUI based interface. Such flexible platform should allow following changes through GUI interface rather than coding <ul style="list-style-type: none"> - Create new or changes to existing - applications and Solutions, - campaigns and surveys - notifications - workflows - change appearance. 		
6	The system should have ability to configure reference and audit data feeds from various sources (scheduled, regular and onetime). The system should provide ability to centralize data from trusted sources in a searchable, standards-compliant database and should not require coding skills to build these integrations. This will enable continuous audit of controls compliance of which can be checked in an automated manner		
7	System should provide flexible application development platform to develop new applications and change existing ones, make changes to, workflows, adhoc reports dashboards, notifications, changing appearance in a code free manner from single interface.		
8	Platform should allow seamless migration of data, application custom development and integration from one environment to another		
9	Flexible integration utilities should be available so as to ensure new integrations can be built and scheduled quickly. The solution should seamlessly integrate with current set of tools used in UIDAI		
10	Solution should provide its own reporting engine without having to rely on any additional third party reporting tool for UID reporting requirements		
Technical Architecture			
12	System should support data export and import formats such as .txt, .csv .xml etc.		



RFP for the Selection of the GRCP-SP

13	System should provide ability to create report in following formats .doc, .pdf, .xls, .csv		
14	System should be able to easily export and import of the applications in order to rolled forward customizations or configurations in an upgrade		
15	UID should be able to use GRC Application virtualised environment if it so desires		
	Access Control		
16	System should <ul style="list-style-type: none"> • support role-based user privileges • support administrator-defined user roles • support granular access controls • keep a record of administrative activities /configuration changes • support single sign on (SSO) 		
	Reporting		
17	System should <ul style="list-style-type: none"> • provide a search engine that allows users to perform simple keyword • provide the ability to save searches as global and personal reports and as charts in multiple formats (i.e., bar, pie, donut, radar and gauge format). Report should be automatically updated every time query is fired. (i.e. Dynamic reports not static reports) • searches as well as complex multi-application searches (controlled by access rights) • support role-based dashboards, views and information access • support custom dashboards (e.g., My Dashboard) • include a wizard-based dashboard creation and editing tool • support rollup reporting with drill-down capabilities • include standard report templates • support custom reports • include a wizard-driven interface to define custom reports • allow reports generation on schedule and on demand • Specific reports should be automatically generated and distributed 		



RFP for the Selection of the GRCP-SP

	via configuration settings • have ability to send alerts on specific thresholds for data or trends.		
	Workflow		
18	System should provide a workflow engine that easily allows users to set up and maintain defined workflow management processes (customizable workflows)		
19	System should support automation of workflow events (e.g., automatic permissioning of records based on record content, show/hide of fields based on record content, etc.)		
20	System should provide a notification engine that allows users to receive email alerts in various stages of the workflow process		
	UID Enterprise Hierarchy and Asset Management		
21	UID should be able to define their own Business and Asset Hierarchy. This entity hierarchical definition should be flexible and should enable the establishment of asset relationships (e.g., relating devices to the branch where they are housed). - Reporting Targets: e.g. Company profiles, Functions profiles, Product Areas profiles, - Evaluation Targets: e.g. Products and services, Business processes, Devices, Applications, Facilities and Personnel. - Geographical Hierarchy : Spoke, Branch, Region, Zone, Corporate etc.		
22	System should support online asset classification by Branch, Function, department, products, Business Processes and Geographies (Spoke, Region, Zone etc.) owners based on rating attributes - Criticality rating - Branch Rating - Confidentiality and Integrity Ratings - ITCM related Availability ratings		



RFP for the Selection of the GRCP-SP

23	The system should consolidate the Risks, Audit Observations, and incidents, Loss events which in turn should be mapped with Applications, Business processes, and branches if applicable. The system should relate assets they affect, enabling the prioritization of patches or workarounds based on asset criticality.		
25	System should provide the ability to rate business area /function based on the risk of incidents reported against it. System should provide ability to roll up the rating further up the business hierarchy defined by UID e.g. department , branch, company level		
	Incident Management		
	Incident Reporting		
26	Automation of Incidents Management System should provide ability – reduce initial response time on incidents identified – Ability to Manage Incidents /loss events from various sources in a single store and tie it back to risks , – Ability to Manage automated compliance checking issues, threats and vulnerabilities on single dashboard		
27	The system should capture incidents of any type, including Incidents (through referrals or sampling) physical incidents (e.g. regulatory Sweep, theft, destruction, lost packages, unauthorized access, etc.) and IT incidents (e.g. IT management, IT Security, malware, etc.). The system should provide - seamless configuration interface to capture additional incident types and other data points - ability to submit incidents on a web-based interface and acquire through other systems		
28	Ability to attach incidents to relevant Targets of Evaluation (Branch, Function, department, products, Business Processes and Geographies (Spoke, Region, Zone etc.))and targets of reporting (Businesses, compliance units)		
29	Provide single view of all the past incidents reported against a target (Branch, Function, department, products, Business Processes and Geographies (Spoke, Region, Zone etc.)) and ability to notify		



RFP for the Selection of the GRCP-SP

	repeat incidents		
30	Incidents Management Systems should provide ability to store pre-determined response procedures and reuse it for similar incidents		
31	Incidents Management System Should provide - Ability to manage and track and evaluate performance of investigation internal teams / vendor team involved through relevant TurnAround Time (TAT) reports such as time taken to close, number of open incidents for more than one day etc. - Ability to provide configurable workflow which can leverage to involve Business owners, IT, etc. in an incident resolution exercise		
Investigation Management			
32	System, should provide ability to • Attach documents, images, audio files, videos and other files to records (Risk, Compliance, Incidents, threats, remediation, findings etc.) as evidence. • Relating Incident to risk and violated policies and controls. • Configure through a graphical user interface, workflow for reporting, assigning, investigating and closing incidents. • Allow creation of library of predefined response procedures that can be categorized by incident type and automatically assigned as incidents are reported. • assign incidents to specific users and response teams, and access to incident data to be restricted to only those users. • Assign Incidents to functional groups and geographical location. • Auto-notified via email Investigators when incidents are reported to which they are assigned. • Allow Multiple investigators can work on a single incident, and track changes made to incident data with a user/date/time stamp. • Relate Potentially "like" incidents. • track court-ordered recovery and restitution payments.		
Reporting for Incidents Management			
33	The system should provide investigators with a dashboard interface for reviewing assigned incidents, adding case notes and attachments		



RFP for the Selection of the GRCP-SP

	and tracking tasks.		
34	The system should provide capabilities to run both ad hoc and standardized reports for operational and trending metrics.		
35	The system should support comparative analysis of incident data.		
36	Facility for all reports to be exported to Word, Excel and PDF.		
	Risk Management		
	Risk Identification: Online risk and compliance Assessments		
37	<p>The system should support risk assessment processes, time and event based notifications and workflow.</p> <ul style="list-style-type: none"> - The system should allow - to quickly build targeted questionnaires through a wizard-driven interface. - Sending reminder and escalation notifications as an assessment due date approaches or is past. - The system supports dynamic surveys (next questions driven by prior response). 		
38	<p>The system should support online risk and compliance assessments which can be portable offline. Such assessment should support:</p> <ul style="list-style-type: none"> - Configurable assessment templates for <ul style="list-style-type: none"> - Online Fraud Assessments - Application Assessments - Information Assessments - Device Assessments - Facility Assessments 		
39	<p>The system should support a master library of questions, linked with control standards that can be used in multiple questionnaires and are mapped to standards / frameworks. System should allow</p> <ul style="list-style-type: none"> - Answers to assessment questions which should trigger automatic finding creation - applying weight to questions and responses. 		



RFP for the Selection of the GRCP-SP

	Risk Measurement		
40	<p>The system should enable COSO ERM implementation allowing to calculate, displays and reports risk scores. These risk calculations should:</p> <ul style="list-style-type: none"> - transparent (no "black box" magic). <ul style="list-style-type: none"> - Users full control over risk calculation parameters, weightings - supports custom risk assessment methodologies and algorithms - aggregate risk scores for any entity or group. <p>The system should allow risk score and compliance score pairs and map these to a maturity model.</p>		
41	System should support monitoring of controls with in compliance assessment at the same time should allow to build KRIs and KPIs to build early warning system		
42	<p>System should allow measurement probability and impact (Likelihood and Consequences) and ability to tie up following with risk :</p> <ul style="list-style-type: none"> - KRIs and KPIs - Loss Events - Incidents - Risk Appetite 		
	Audit Management		
	Audit Universe		
43	<p>The system should allow UID to use various types of auditable entities:</p> <p>Business processes</p> <p>Facilities</p> <p>Third parties</p> <p>Applications</p> <p>Other</p>		
44	<p>The system should provide ability to perform online assessments of the audit universe to</p> <ul style="list-style-type: none"> - determine inherent and control risk associated with each audit entity. 		



RFP for the Selection of the GRCP-SP

	- determine audit scope.		
	Audit Project Management		
45	The system should provide ability to maintain a library of procedures that can be used in the context of multiple audit projects. Procedures can be assigned to audit projects automatically or ad hoc.		
46	The system should automatically generate - work papers for each audit project. - email notifications to alert audit staff of their tasks.		
50	The system should support calendar display of audit staffing.		
51	The system should be available to audit staff regardless of their location.		
52	The system should provide tiered access control to various levels of audit staff.		
53	The system should support multiple audit projects simultaneously.		
	Audit Execution		
54	The system should provide flexible workflow capabilities to match the type of audit project.		
55	The system should capture the results of audit tests within work papers.		
56	The system should provide electronic storage, tracking, management and control of work papers.		
57	The system should provide the ability to attach supporting documentation and review notes to work papers.		
58	The system should provide the ability to incorporate data from work papers into an audit report.		
59	The system should track milestones in the audit process, including kick-off meetings and field work.		
60	The solution should capture meta data for users that flag milestones complete.		
61	The system should provide the ability to export and import data to and from standard data formats.		



RFP for the Selection of the GRCP-SP

	Deficiency Management		
62	The system should generate findings automatically when failures are noted in audit testing.		
63	The system should enable audit customers to respond to noted findings through an online portal.		
64	The system should be able to automatically route findings to responsible personnel for management.		
65	The system should allow to manage findings through acceptance, remediation tasks or exception requests.		
66	The system should provides task management capabilities for creating, assigning and tracking tasks.		
67	The system should provide task management capabilities and capture a history of all changes to records and the user who made them.		
	Reporting		
68	The system should support tracking and reporting of the entire audit lifecycle.		
69	The system should provide audit staff with a dashboard interface for reviewing assigned tasks and adding notes and attachments.		
70	The System should support automatic summary report generation		
	Crisis Management		
71	The system should capture crisis events of any type.		
72	The system should provide a point-and-click configuration interface to capture additional event types and other data points.		
73	Crisis event reporting should be web-based and accessible via geographically dispersed operating units. Should have Access by internal employees and Secure access for external employees		
74	The system should supports crisis event reporting via manual data entry by a call center representative or employees.		
75	The system should support integration with a call center or notification service.		
76	IT continuity and disaster recovery plans should be linked to crisis events and invoked from within the crisis management interface.		



RFP for the Selection of the GRCP-SP

77	The system should track the implementation of IT continuity and disaster recovery plans.		
78	The system should support loss and recovery tracking.		
Governance, Risk and Compliance Integration			
79	The system should be able to tie IT-Compliance data to enterprise management assets such as business processes, applications, devices, facilities, and critical business information to derive impacts when an event occurs.		
80	The system should connect crisis event data with incident management capabilities tying recovery efforts to incidents and investigations.		
81	The system should be able to relate business continuity and disaster recovery plans to specific vendors enabling the organization to inform third-party suppliers that a crisis event may impact their ability to exchange information or provide services to the organization. It also enables effective management of threats resulting from vendor relationships.		
Policy Management			
82	<p>The system should support creation, management and importing/exporting policies, controls and technical baselines. The system should control content library with mapping to industry best practices, framework, regulations and standards including but not limited to following and should allow users to map newer regulations and compliances to Control Library:</p> <ul style="list-style-type: none"> - ISO 27001 and ISO 27002 - CoBIT 4.1 / 5 - PCI DSS 1.2 - ITIL - NIST Pub 800 - BS25777 		

83	<p>The system should support Control content library which include policies, controls Standards, and Control Procedures technical Baselines library for technologies used by Organization. Technical Control procedures should provide implementation and assessment guidance. Technical baselines must be written against control standards and mapped to regulatory requirements. Such control library should include all the control procedures required for following:</p> <ul style="list-style-type: none"> - ISO 27001 and ISO 27002 - CoBIT 4.1 / 5 - PCI DSS 1.2 - ITIL - NIST Pub 800 - BS25777 		
84	<p>System should employ real-time reports and dashboards to give enterprise view of policies and control standards mapped to regulatory requirements, identify gaps between policies and authoritative sources, and monitor policy exceptions enterprise-wide.</p> <ul style="list-style-type: none"> - The system should support the monitoring and reporting the organisation's compliance levels at control procedures, control standard, policies and company objective levels. - The System Should Support monitoring and reporting control compliance levels at Business unit level and roll-up to Division, Company and Group level with ability to configure additional Hierarchy levels - The system should generate real-time reports and user-specific dashboards to provide visibility into the status of assessment efforts and the organization's overall risk profile. 		
85	<p>System should automatically roll up level of compliance at each control level and business hierarchy level and should flow from the downstream compliance assessments.</p>		



RFP for the Selection of the GRCP-SP

86	<p>The system should</p> <ul style="list-style-type: none"> • support submission of time-limited policy exception requests. • support exception request review and approval workflow. • track end of exception period and will notify relevant parties in advance. • log the lifecycle of authorized exceptions. 		
87	<p>The system should supports policy authoring and content review workflows and approval work flow with ability to configure additional levels if required.</p> <p>.</p>		
	Compliance Management		
88	Ability to define time based and event based compliances with ability to assess on time/ event triggers.		
89	System should allow scoping controls for business unit and business process and ability to define key controls		
90	System should allow Compliance assessment through fully reconfigurable questionnaires		
91	<p>System should support following l:</p> <ul style="list-style-type: none"> - Risk and Compliance Matrix - Control self-assessment capability - Testing of Controls <ul style="list-style-type: none"> - Testing Plans - Test of Design - Test of effectiveness 		
92	<p>System should allow following:</p> <ul style="list-style-type: none"> - Maintain automated technical compliance checking (e.g. Compliance Scans) - Manual testing of technical controls - Testing of process controls 		
	Compliance Scoring and Gap Analysis		
93	The system's compliance scores should seamlessly combine survey-based and automated testing results and data from third-party tools.		
94	The system should flag result discrepancies (e.g., between survey-		



RFP for the Selection of the GRCP-SP

	based and automated test results).		
95	The system should calculate compliance scores for each regulation.		
96	The system should calculate aggregate compliance scores for multiple regulations.		
97	The system should allow calculation of compliance scores for any group, including dynamically defined groups.		
	Threat Management		
99	The system should centralize threat data from trusted sources in a searchable, standards-compliant database.		
100	The system's database should require no specialized administration skills.		
101	Threat definition should be flexible and include:		
102	Vulnerabilities		
103	Malicious code		
104	Geopolitical threats		
105	Patches		
106	The system should be pre-integrated with security intelligence feeds (e.g., iDEFENSE, Symantec DeepSight, iSIGHT Partners IntelliSIGHT, etc.)		
107	The system can be populated with threat data from email advisories.		
108	The system should be able to consolidate the results of multiple network scans and links those results directly to physical assets.		
109	The system should be able to relate threats to the assets they affect, enabling the prioritization of patches or workarounds based on asset criticality.		
	Remediation Management		
110	The system automatically notifies personnel when threats are identified on assets for which they are responsible.		
111	Notifications should include details on the severity of the threat, the CVE ID, affected technologies and remediation instructions.		
112	Notifications should include links to the full threat and patch		



RFP for the Selection of the GRCP-SP

	records.		
113	The system should support threat remediation through mitigation or acceptance.		
114	The system should provide task management capabilities for creating, assigning and tracking tasks.		
115	Task management capabilities should capture a history of all changes and the user who made them.		
Reporting			
116	The system should provide a set of predefined reports (e.g., vulnerabilities by type or severity level, malicious code by type, remediation tasks by status, etc.).		
117	The system should provide the ability to produce ad hoc reports to view threats by technology, severity, type and impact to the organization.		

12.6. Fraud detection

The fraud detection and management sub-system will have the following key components:

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response: How do you comply with this requirement? Or What is missing to achieve the compliance?
1	Rules Engine - Maintain fraud pattern definitions and their corresponding counter-measure work flows. As and when new patterns of fraud are determined, they shall be updated into the Rules Engine without requiring a software release.		
2	Work Flow Engine - This would be the core engine that would direct the fraud management actions through a well-defined set of steps as defined in the work flow template (to be defined by GRCP-SP) for the fraud pattern. The Rules Engine will define the fraud pattern and then point the system to run the corresponding "Counter-Measure work flow". This work flow will also be updated along with updation of Rules without requiring a software release and hence would ensure ease of maintenance and expansion.		
3	Queue Management & Assignment - This component would take care of assigning the fraud patterns based on their severity and applicability to appropriate management staff in the NOC. It will support maintaining different queues for each operations group and associating people to the queue, so that assignment happens to the appropriate individual who is assigned to the queue. It will also take care of distributing the tasks amongst the available manpower assigned to the queue.		

GRCP-SP shall ensure a tight integration and optimal use of the infrastructure, tools and facilities that are set-up in the STARMC including Forensics Lab and the Fraud Risk Management platform brought in by MSP / ecosystem partners.

12.7. Risk Simulation

Sl No	Requirement Description	Indicate the Following: 1=Compliant 2=Non-Compliant	Please Explain your response : How do you comply with this requirement ? Or What is missing to achieve the compliance ?
1	The system should be capable to support discrete event, system dynamics, and agent based modeling		
2	The system should support development of Hybrid / Multi-Paradigm Simulations		
3	Should have easy to use graphical interface for building complex models		
4	It should have models that can run on any platform		
5	The system should automatically create web ready simulations/models, distribute web based applets at no additional cost and should have no need to install any extra software.		
6	The system should have the ability to quickly understand the risk impact of proposed changes to a network's configuration before the changes are implemented on the actual network, hence minimizing the time to roll out new applications and services		

12.8. Indoor LED video wall specifications:

An indoor LED video wall with the below Minimum specifications should be proposed as part of the technical proposal and costing for the same should be done as a separate line item for both DC and DR in the financial proposal.

Sl No	Item	Specifications
1	Pixel Pitch (mm)	8 or less
2	Configuration (LED)	LED for every Primary Color (per module)
3	Resolution(pixels/M2)	17000 or more.
4	Module size	The size of the wall to be covered is [3 meters X 1.5 meters]. Modules to be provided by the vendor, as per their available module size, to cover the wall.
5	Cabinet size	To be customized as per requirement.
6	Viewing angle (V*H)	140*140 or more
7	Brightness (cd)	>=4000 (for complete wall)
8	Max power required	Upto 250 watts per module.
9	Refresh rate (Htz)	> =300
10	Input sources	S-video, composite, YUV, RGB, SDI, HDSDI, Data DVI up to UXGA. Network streaming support over LAN, Full HD support.
11	Output media	All formats of video, image, flash, power point, dynamic content like TV, RSS feed, web pages, micro blog, embedded HTML.
12.	Video format	Mpeg, jpeg, avi, flv, 3gpp2, agp and mov.
13	Control system	Synchronized with PC controller
14	Life time	More than 50,000 Hrs
15	Management Software	Video wall should have a wall management software and display 4 universal inputs of variable size.

12.9. Additional components to be brought in by GRCP-SP for STARMC:

Following are the additional components that need to be brought in by GRCP-SP as part of setting up of STARMC. Cost for these components shall be loaded at uniform rate across all bidders for the purpose of evaluation of commercial bids (to the tune of INR 2 Crore) However, the payment for the same shall be at actuals subject to approvals by UIDAI. UIDAI reserves the right to route the procurement and implementation of following items either through selected GRCP-SP or through any other party.

- UPS
- Fire suppression system
- Generator
- Servers and network equipment which will be rack mountable and each rack will be hosted in cage
- Desktops
- Plasma screens - separate for air gapped
- A/C
- False flooring
- Access control for cages and entrance
- Biometric access

UIDAI shall provide the physical site for setting up the STARMC including forensics lab. The GRCP-SP shall be responsible for all site preparation activities and for setting up STARMC including forensics lab.

13. Key Personnel

The GRCP-SP resources will be required to work onsite at the UIDAI office premises or as required for the project as decided by DDG (Technology). The Bidder's company shall take the complete responsibility to bring in other resources (not mentioned below) as and when required to execute the Design and implementation of the GRC Framework, 24*7 security monitoring operations, fraud and forensics, and providing Performance Assurance Services as per the contract. The envisaged critical members of the GRCP-SP's indicative team structure are given below. Key personnel specified below shall be firm committed resources for this project and GRCP-SP shall not substitute these resources for deployment on the project. No replacements are allowed for key personnel proposed as part of the Design and Implementation phase for the first six months of the project. No replacements are allowed for key personnel proposed as part of the Operations phase for the first six months of the operations phase.

Profile 1: Project Director		
1.	Role in the Project:	Shall be responsible for managing the complete program and the team. Shall take ownership of entire scope of work as defined in this RFP. This person will be the nodal point of communication with UIDAI
2.	Area of Expertise:	Ability to interact with Board members in a business language to explain the risks, business impact and mitigation strategies and with the GRCP team in a technical language to explain the controls and monitoring strategies.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Should be an experienced program manager. Professional qualification: PMP / CISM / CGRC-IT certification or equivalent (desirable).
5.	Professional Experience:	1) 15+ years of overall experience with at least 10 years of relevant experience in managing all aspects of a large advisory/ program management 2) Must have experience in managing at least 5 completed projects for large, enterprise scale Clients in GRCP related advisory work. 3) Should have GRCP Framework based work delivery for government clients globally.

6.	Expected involvement in the project:	Full time
----	---	-----------

Profile 2: Program Manager		
1.	Role in the Project:	Shall be responsible for managing the complete program and the team. Shall take ownership of entire scope of work as defined in this RFP. This person will be the nodal point of communication with UIDAI
2.	Area of Expertise:	Ability to interact with Board members in a business language to explain the risks, business impact and mitigation strategies and with the GRCP team in a technical language to explain the controls and monitoring strategies.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Should be an experienced program manager. Professional qualification: PMP / CISM / CGRC-IT certification or equivalent (desirable).
5.	Professional Experience:	1) 10+ years of overall experience with at least 10 years of relevant experience in managing all aspects of a large advisory/ program management 2) Must have experience in managing at least 5 completed projects for large, enterprise scale Clients in GRCP related advisory work. 3) Should have GRCP Framework based work delivery for government clients globally.
6.	Expected involvement in the project:	Full time

Profile 3 - Governance: Governance Senior Consultant		
1.	Role in the Project:	Shall be responsible for establishing and maintaining governing policies, organization structure, processes and procedures, reporting standards, communication channels and escalation procedures.
2.	Area of Expertise:	IT Governance expert with analytical skills to understand patterns, trends, technical reports, findings

		and translate them to business language in relation to process, technology and people
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M.Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. Preferable: CGRC-IT / CISM / CRISC/ CISSP / GIAC certification or equivalent.
5.	Professional Experience:	1) At least 5 years of relevant experience in managing governance aspects of IT Security advisory and audit project 2) Should have performed GRCP based governance services for clients during his/her career with a successful track record.
6.	Expected involvement in the project:	Full time

Profile 4- Risk: Risk and Incident Manager

1.	Role in the Project:	Responsible for coordinating, in a timely manner, all activities necessary for risk management, analyzing incidents / risks, incident / risk containment, identifying root cause, initiate problem resolution, incident / risk response and communication
2.	Area of Expertise:	Incident management, change management , problem management and ability to work 24x7 during crisis
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Should be an experienced IT Security practitioner. Preferable: CITR / CIRM / CISSP/CRISC/ CISM/GIAC / GCIH certification or equivalent
5.	Professional Experience:	1) 10+ years of overall experience with at least 5 years of relevant experience in managing all aspects of risk and incident analysis. 2) Should have competence required to competently manage the Incident Management ITILv3 process

		3) Must have experience in managing at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 5- Risk: Risk Simulation Analyst

1.	Role in the Project:	Responsible for conducting all activities necessary for risk modeling, simulation and conduct analysis to throw insights on simulated scenarios
2.	Area of Expertise:	Well versed with multiple risk modeling and simulation tools and techniques
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M.Tech / MBA / PhD degree or equivalent. Preferable: CIRM / CRISC / CITR / CISSP / CISM certification or equivalent
5.	Professional Experience:	1) 5+ years of overall experience with at least 3 years of relevant experience in managing all aspects of risk modeling and simulations. 2) Must have experience of conducting risk modeling and simulation analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 6- Risk: Pattern Analyst

1.	Role in the Project:	Responsible for conducting all activities necessary for risk pattern analysis and conduct analysis from the patterns to throw insights on past, present and future scenarios
2.	Area of Expertise:	Should have a keen eye and analytical mind to see existing and emerging patterns with the ability to translate them to business risks and opportunities to carry out proactive mitigations. Should be able to look at a vast array of unstructured digital data and derive value out of it using predictive analytics.

3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M.Tech / MBA / PhD degree or equivalent. Preferable: CIRM / CRISC / CITR / CISSP / CISM / CBP / CBSE certification or equivalent
5.	Professional Experience:	1) 5+ years of overall experience with at least 3 years of relevant experience in managing various aspects of pattern analysis. 2) Must have experience of conducting pattern analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 7- Risk: Risk Analyst		
1.	Role in the Project:	Responsible for conducting all analysis activities necessary for risk identification, assessment, response, profiling, controls and communication
2.	Area of Expertise:	Ability to analyse technical and business risks related to security and privacy by taking into consideration multiple, global and local, trends and inputs
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent. Preferable: CIRM / CRISC / CITR / CISSP / CISM / CBCP / GIAC / CIRCP / CIPP/IT certification or equivalent
5.	Professional Experience:	1) 7+ years of overall experience with at least 3 years of relevant experience in managing all aspects of risk analysis. 2) Must have experience of conducting risk analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 8- Risk: Fraud Analyst		
1.	Role in the Project:	Responsible for identifying fraud and conducting all analysis activities necessary for fraud management
2.	Area of Expertise:	Should be a seasoned fraud analyst / examiner and should have experience in handling frauds across multiple industry domains. Should be able to identify and look at a vast array of unstructured data to identify possible fraud and fraud patterns.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech/B.S / MCA / M.Tech / MBA degree or equivalent. Preferable: CFS/CEH/ GIAC/ GWAPT/ GWEB/ GXPN/ GPEN certification or equivalent.
5.	Professional Experience:	1) 7+ years of overall experience with at least 3 years of relevant experience in all aspects of fraud management analysis. 2) Must have experience of conducting fraud management analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 9- Periodic Compliance : Periodic Compliance Manager		
1.	Role in the Project:	Shall be responsible for managing the complete periodic compliance program and the corresponding team. Shall take ownership of entire scope of periodic compliance as defined in this RFP.
2.	Area of Expertise:	Ability to draw up compliance schedules, compliance checklists to be followed, carrying out compliance and penetration tests, ensuring follow up for closure of identified gaps in terms of deficiencies and deviations, ensuring a regular maturity trend, keeping the team motivated
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech/B.S / MCA/ M. Tech / MBA degree or equivalent. Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISA/ CISM/ CISSP / CBCP / DRCS / CISRCP / CAST / GIAC/

		CSCS / CBP / CBSE/ GPEN / GWAPT / GWEB / CASS / CIPP/IT certification or equivalent.
5.	Professional Experience:	<p>1) 10+ years of overall experience with at least 7 years of relevant experience in managing all aspects of audit.</p> <p>2) This includes application audit, network and security audit, hardware audit, project management of the audit (includes monitoring, scheduling, follow up for closure, etc.), testing of controls, ensuring controls coherence, developing test cases for controls, management of audit resources.</p> <p>3) Must have experience in managing at least 3 completed projects for large, enterprise scale Clients in audit.</p> <p>4) Should have GRCP Framework based auditing experience in at least 2 projects</p>
6.	Expected involvement in the project:	Full time

Profile 10- Periodic Compliance : Network Security Auditor

1.	Role in the Project:	Shall be responsible for managing the complete network security audit hands-on and shall take ownership of entire scope of the network audit.
2.	Area of Expertise:	Deep understanding of network security, protection of networks using controls related to people process and technology, well versed with various tools used for protection of networks and related components from a security perspective
3.	Number of Resources (Minimum Requirements):	2
4.	Educational Qualifications:	B.E/B. Tech / B.S / MCA / MBA/ M. Tech degree or equivalent. Should be a certified auditor. Preferable: CISSP / BS7799 Lead Auditor/ CISM/CEH / GPEN/ GCFW/ CCNA/ CCNP/ CCSE / CCSA certification or equivalent
5.	Professional Experience:	1) At least 7+ years of experience in managing audit of countrywide / large networks.

		<p>2) Shall have expertise in auditing network equipment (including routers, switches, firewalls, LAN/WAN components etc.) against the bill of material and specifications.</p> <p>3) Shall have expertise in audit of the network deployment against the defined network architecture post the commissioning of the network by the vendor. Excellent knowledge of OSI Model, TCP/IP protocol suite (IP, ARP, CMP, TCP, UDP, SNMP, FTP)</p> <p>4) Must have experience in at least 3 completed projects for large, enterprise scale Clients in the above mentioned audit areas.</p>
6.	Expected involvement in the project:	Full time

Profile 11- Periodic Compliance : Application Security Auditor

1.	Role in the Project:	Shall be responsible for managing the application security and web security audit/assessment hands-on and shall take ownership of entire scope of the application assessment
2.	Area of Expertise:	Excellent understanding of application security and privacy impact assessment in each phase of the software development lifecycle, excellent understanding in Java security
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech / B.S / MCA / M. Tech / MBA degree or equivalent Should be a certified auditor. Preferable: GWEB / CASS / GWAPT/ BS7799 Lead Auditor/ CISM / CISSP / CCSK / CIPP/IT certification or equivalent.
5.	Professional Experience:	<p>1) At least 5+ years of experience in managing software and web application assessments.</p> <p>2) Shall have expertise in SDLC, software and web applications assessment.</p> <p>3) This includes audit against functional requirements</p>

		and audit against technical architecture for compliance to it. 4) Must have experience in at least 3 completed projects for large, enterprise scale Clients in the above mentioned areas.
6.	Expected involvement in the project:	Full time

Profile 12- Periodic Compliance : Database Security Auditor		
1.	Role in the Project:	Shall be responsible for managing the database security audit/assessment hands-on and shall take ownership of entire scope of the database security assessment
2.	Area of Expertise:	Well versed with aspects of database security and privacy, access control, identity management, biometric storage, encryption of database, data obfuscation techniques. Has deep security related knowledge of Oracle, My SQL and SQL databases.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent Should be a certified auditor. Preferable: BS7799 Lead Auditor/ CISSP / CISM / CISA/ CDRP/ CIRM / CBP / CBSE / CIPP/IT certification or equivalent.
5.	Professional Experience:	1) At least 5+ years of experience in managing database security and privacy assessment. 3) This includes audit against functional requirements and audit against technical architecture for compliance to it. 4) Must have experience in at least 3 completed projects for large, enterprise scale Clients in the above mentioned areas.
6.	Expected involvement in the project:	Full time

Profile 13- Periodic Compliance : OS Security Auditor		
1.	Role in the Project:	Shall be responsible for managing the operating systems and system software audit/assessment hands-on and shall take ownership of entire scope of the operating systems and system software security assessment
2.	Area of Expertise:	Is well versed with security aspects of Unix and its various flavors and with Microsoft operating systems.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent Should be a certified auditor. Preferable: CISSP / CISM / BS7799 Lead Auditor/ CISA/ GCUX/ RHCSS/ CWSS/ MCSE / MCSA / CIPP/IT certification or equivalent.
5.	Professional Experience:	1) At least 5+ years of experience in managing operating systems security assessment and hardening of systems. 3) This includes audit against functional requirements and audit against technical architecture for compliance to it. 4) Must have experience in at least 3 completed projects for large, enterprise scale Clients in the above mentioned areas.
6.	Expected involvement in the project:	Full time

Profile 14- Periodic Compliance : Privacy Auditor		
1.	Role in the Project:	Shall be responsible for managing the operating systems audit/assessment hands-on and shall take ownership of entire scope of the information privacy assessment
2.	Area of Expertise:	Well versed with privacy impact assessments at system software level, application level, web and cloud level, database level, access control level. Well versed with various Privacy related global laws, best practices, emerging directions in policies
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E/B. Tech / B.S MCA / MBA / M. Tech degree or

		equivalent Should be a certified auditor. Preferable: CIPP/IT / CISM / CISSP / BS7799 Lead Auditor/CISA/CEH/ CREA/ CASS / RHCSS/ CIRM/ GIAC/ GPEN/ GCUX/ MCSE certification or equivalent.
5.	Professional Experience:	1) At least 5+ years of experience in managing information privacy and privacy impact assessments. 3) This includes audit against functional requirements and audit against technical architecture for compliance to it. 4) Must have experience in at least 3 completed projects for large, enterprise scale Clients in the above mentioned areas.
6.	Expected involvement in the project:	Full time

Profile 15- Periodic Compliance : Forensics Analyst

1.	Role in the Project:	Shall be responsible for assessing and investigating escalated security breach incidents.
2.	Area of Expertise:	Is well versed with evidence handling and storage of data including volatile data during investigations, email tracing, disk imaging, recovery of deleted files / fragments of data / passwords and forensic data collection and analysis, preparing witness testimony and support during litigations, able to carry out malware and steganography analysis, identifying phishing sites and their takedown, recreation of time critical events, network session analysis and extracting files from sessions, database forensics, collaborating with law enforcement for investigations, civil injunctions or search orders, has clear understanding of the law, IT Act, RTI, etc., has worked with multiple forensic related tools
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent. Should be an experienced Computer Forensics/



RFP for the Selection of the GRCP-SP

		Investigative Response practitioner. Preferable: SANS CSFA / GCFE/ GREM / GREA / CHFI / DRCS / Encase Certified/ CDRP/ GCIA / SANS Incident Handler certification or equivalent.
5.	Professional Experience:	1) Fulltime - At least 7 years of computer forensics work experience. Should be well conversant with forensic tools and setting up forensic labs, has relations with law enforcement 2) On demand Expert - Should have at least 10+ years of computer forensics, Investigative Response experience for at least 10+ global investigations in the area of expertise.
6.	Expected involvement in the project:	Full time

Profile 16- 24*7 Compliance : STARMC Manger

1.	Role in the Project:	Shall be responsible for managing overall operations for the STARMC center.
2.	Area of Expertise:	Has experience of 24x7 security operations to monitor and manage states and events (of devices, services, software) at host, network and application level by correlating logs, vulnerabilities, configurations, assets, patches, performance and network behavioral anomaly data and collaborating with the various stake holders in the eco system. Should be well versed with service delivery / ITIL.
3.	Number of Resources (Minimum Requirements):	2
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent. Should be an experienced Security Operations / Managed Security Services practitioner. Preferable: CISM/CISSP certification or equivalent.
5.	Professional Experience:	1) At least 8 years of relevant experience in managing STARMC aspects of a Security project 2) Should have performed GRCP based Services for clients during his/her career with a successful track record.

6.	Expected involvement in the project:	Full Time
----	--------------------------------------	-----------

Profile 17- 24*7 Compliance : Malware Analyst

1.	Role in the Project:	Responsible for conducting all analysis activities necessary for malware identification, mitigation and simulation
2.	Area of Expertise:	Hands on experience in identification of malware, reverse engineering of malware, containment of malware, well aware of malware trends and vulnerable digital assets that the malware could exploit.
3.	Number of Resources (Minimum Requirements):	1
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent. Preferable: GREM / CEH/ CREA/ GIAC/ GCUX/ GXPEN certification or equivalent
5.	Professional Experience:	1) 5+ years of overall experience with at least 3 years of relevant experience in managing all aspects of malware analysis. 2) Must have experience of conducting malware analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 18- 24*7 Compliance : Network Security Analyst (24*7)

1.	Role in the Project:	Responsible for conducting all analysis activities necessary for network security analysis
2.	Area of Expertise:	Deep understanding of network security, designing secure networks, protection of networks using controls related to technology, well versed with various tools used for protection of networks and related components from a security perspective. Well versed with ITIL.
3.	Number of Resources (Minimum Requirements):	3
4.	Educational Qualifications:	B.E/B. Tech / B.S / MCA / MBA/ M. Tech degree or equivalent. Should be a certified auditor.

		Preferable: CISSP / BS7799 Lead Auditor/ CISM/CEH / GPEN/ GCFW/ CCNA/ CCNP/ CCSE / CCSA certification or equivalent
5.	Professional Experience:	<p>1) 5+ years of overall experience with at least 3 years of relevant experience in managing all aspects of network security analysis.</p> <p>2) Shall have expertise in setting up and maintaining secure and hardened network equipment (including routers, switches, firewalls, LAN/WAN components etc.).</p> <p>3) Shall have expertise in setting up and maintaining a secure and hardened network against the defined network architecture.</p> <p>4) Must have experience of conducting network security analysis for at least 3 projects for large, enterprise scale Clients.</p>
6.	Expected involvement in the project:	Full time

Profile 19- 24*7 Compliance : Correlation Analyst (24*7)

1.	Role in the Project:	Responsible for conducting all analysis activities necessary for log correlation
2.	Area of Expertise:	Should be able to manage states and events (of devices, services, software) at host, network and application level by correlating logs, vulnerabilities, configurations, assets, patches, performance and network behavioral anomaly data
3.	Number of Resources (Minimum Requirements):	3
4.	Educational Qualifications:	<p>B.E. / B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent.</p> <p>Preferable: CISSP / CEH/ CREA/CCSA/ RHCSS/ GIAC/ GWAPT/ GWEB/ CASS / GXPN/ GCFW/ GCUX/ CDRP/ CCSK/ GPEN GXPN/ GCFE certification or equivalent</p>
5.	Professional Experience:	1) 5+ years of overall experience with at least 3 years of relevant experience in managing all aspects of correlation analysis.

		2) Must have experience of conducting correlation analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 20- 24*7 Compliance : Monitoring Expert (24*7)

1.	Role in the Project:	Shall be responsible for monitoring and operating STARMC deliverables.
2.	Area of Expertise:	Should be able to effectively and efficiently monitor states and events (of devices, services, software) at host, network and application. Well versed with ITIL.
3.	Number of Resources (Minimum Requirements):	3
4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA / MBA / M. Tech degree or equivalent. Should be an experienced Security Operations / Managed Security Services practitioner. Preferable: CISSP / ISO 27001/CCSA/ GWAPT/ GWEB/ GXPN/ CCNA/ GIAC/ GCUX certification or equivalent.
5.	Professional Experience:	1) At least 3 years of relevant experience in working for Security monitoring and management operations for Clients. 2) Must have experience of conducting risk analysis for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 21- Performance : Performance Assurance Auditor

1.	Role in the Project:	Responsible for conducting all analysis activities necessary for performance measurement assurance
2.	Area of Expertise:	Well versed with ITIL and excellent understanding of IT Systems performance measurement and related process.
3.	Number of Resources (Minimum Requirements):	1

4.	Educational Qualifications:	B.E. / B. Tech / B.S / MCA degree or equivalent. Preferable: CISA / CISSP / ITIL certification or equivalent
5.	Professional Experience:	1) 5+ years of overall experience with at least 3 years of relevant experience in managing all aspects of performance assurance audits. 2) Must have experience of conducting performance assurance audits for at least 3 projects for large, enterprise scale Clients.
6.	Expected involvement in the project:	Full time

Profile 22- Performance : Project Management Consultants

1.	Role in the Project:	Part of Project management Office working with GRCP-SP Project Director
2.	Area of Expertise:	IT Program and Project Management
3.	Number of Resources (Minimum Requirements):	2
4.	Educational Qualifications:	B.E./B.Tech./MBA degree or equivalent and PMP certification desirable
5.	Professional Experience:	1) 6+ years of overall experience with at least 4 years of relevant experience in managing all aspects of IT program and project management. 2) Work as part of GRCP-SP program management office to provide project management support. Provide analytical support to analyze and report on identified parameters. Manage GRCP-SP reporting and communication. Provide support in issue management and resolution, follow up and report on pending actionable of UIDAI ecosystem partners. Plan and coordinate meetings and follow up on the action items.
6.	Expected involvement in the project:	Full time

List of certifications:

1. CGRC-IT (Certified in IT Governance, Risk Compliance),
2. CITR (Certified in Information Technology Risk Management)
3. CIRM (Certified in Integrated Risk Management)

4. CISA (Certified Information Systems Auditor)
5. CISM (Certified Information Security Manager)
6. CISSP (Certified Information Systems Security Professional)
7. CBP (IEEE Certified Biometrics Professional)
8. CBSE (Certified Biometric Security Engineer)
9. CEH (Certified Ethical Hacker)
10. CHFI (Certified Hacking Forensic Investigator)
11. GIAC (Global Information Assurance Certification)
12. CBCP (Certified Business Continuity Professional)
13. DRCS (Disaster Recovery Certified Specialist)
14. CCSK (Certificate of Cloud Security Knowledge)
15. CSFA (Cyber Security Forensic Analyst)
16. GREM (Reverse Engineering Malware Certification)
17. GCUX (GIAC Certified UNIX Administrator)
18. GCIH (GIAC Certified Incident Handler)
19. GCIA (GIAC Certified Intrusion Analyst)
20. GPEN (GIAC Certified Penetration Tester)
21. GCFW (GIAC certified firewall analyst)
22. GWAPT (GIAC web application penetration tester)
23. GWEB (GIAC Web Application Defender)
24. GXPN (GIAC Exploit Researcher and Advanced Penetration Tester)
25. CCFE (Certified Computer Forensics Expert)
26. CASS (Certified Application Security Specialist)
27. CDRP (Certified Data Recovery Professional)
28. CREA (Certified Reverse Engineering Analyst)
29. CAST (Compliance Assessment & Security Testing)
30. BS7799 Lead Auditor
31. CRISC (Certified in Risk and Information Systems Control)
32. CISRCP (Certified Information Systems Risk and Compliance Professional)
33. CFS (Certified Fraud Specialists)
34. CIRM (Certified Identity Risk Manager)
35. CSCS (Certified Security Compliance Specialist)
36. CIPP/IT (Certified Information Privacy Professional/Information Technology)
37. CWSS (Certified Windows Security Specialist)
38. ITIL (Information Technology Infrastructure Library)
39. CCNA (Cisco Certified Network Associate)
40. CCNP (Cisco Certified Network Professional)
41. CCSE (Check Point Certified Security Expert)
42. CCSA (Check Point Certified Security Administrator)
43. RHCSS (Red Hat Certified Security Specialist)
44. MCSE (Microsoft Certified Systems Engineer)



45. MCSA (Microsoft Certified System Administrator)