



# Certification Framework

May 2023

# Contents

1	Understanding ONDC	5
1.1	Introduction	5
1.2	Participants in the ONDC network	7
1.2.1	User journeys in the ONDC network	10
2	Certification Framework	11
2.1	Guiding Principles	11
2.2	Lenses of Evaluation	13
2.3	Building Blocks of Certification Framework	15
2.4	Levels of Compliance in Certification Framework	20
2.4.1	Need for Levels of Compliance	20
2.4.2	Levels of Compliance Parameters	20
2.4.3	Illustrative Example	21
2.5	Certification Process	22
2.6	Timelines for Evaluation	24
2.7	Different Journeys for Different Participants	25
2.7.1	ONDC Policy Compliance / KYC / Signed Undertaking (as per Law)	25
2.8	Continuous Assessment and On Demand Recertification	26
2.8.1	Continuous Assessment	26
2.8.1.1	Triggers for Continuous Assessment	26
2.8.2	On-Demand Recertification	27
2.8.2.1	Triggers for On-Demand Recertification	27
3	Roles & Responsibilities of Certification Agency	28
3.1	Runbook Update Process Steps	31
3.2	Runbook Update Process example	32
4	Annexures	34
4.1	Annexure 1 – ONDC Policy Compliance Checklist	34
4.2	Annexure 2 – Business Case Scenarios based on APIs	35
4.3	Annexure 3 – Reference Test Cases based on NP/EP Type	37
4.4	Annexure 4 - Assessment Report format	38
4.5	Annexure 5 - ONDC Certificate Data Points	39
4.6	Reference Documents/Links	40

## Table of Figures

Figure 1: ONDC Big Picture .....	6
Figure 2: Type of participants in ONDC network .....	7
Figure 3: Unbundled responsibility of <b>search &amp; discovery</b> on the ONDC network .....	10
Figure 4: Unbundled responsibility of <b>ordering &amp; fulfilment</b> on the ONDC network.....	10
Figure 5: Benefits to the participants and responsibilities of the participants to enable certification framework .....	11
Figure 6: Building blocks of certification framework.....	15
Figure 7: Requirements for different "levels of compliance".....	24
Figure 8: Network Participant Journey .....	25
Figure 9:Ecosystem Participant Journey .....	25
Figure 10: Continuous Evaluation and Re-Certification Workflow.....	27
Figure 11: Process to build the runbook.....	31
Figure 12: ONDC Key APIs.....	35

## Abbreviations

S. No.	Abbreviation	Full Form
1.	BS	Business Scenarios
2.	CA	Certification Agency
3.	CERT-In	Indian Computer Emergency Response Team
4.	EP	Ecosystem Participant
5.	GSTN	Goods and Service Tax Network
6.	IGM	Issue and Grievance Management
7.	ISN	Inventory Seller Node (Inventory-based Seller Side App)
8.	LSP	Logistics Service Provider
9.	MSN	Marketplace Seller Node (Marketplace-based Seller Side App)
10.	NP	Network Participant
11.	ODRSP	Online Dispute Resolution Service Provider
12.	ONDC	Open Network for Digital Commerce
13.	POD	Payment On Delivery
14.	RSP	Reconciliation Service Provider
15.	SMART	Specific, Measurable, Attainable, Relevant and Time-Bound
16.	TC	Test Cases
17.	TS	Test Scenarios
18.	TSP	Technology Service Provider

# 1 Understanding ONDC

## 1.1 Introduction

Open Network for Digital Commerce (ONDC) has been established to revolutionize the digital commerce landscape. ONDC aims to democratize and transform how digital commerce is conducted by introducing a decentralized and unbundled approach to e-commerce.

Traditionally, e-commerce has been dominated by centralized platform models where all functionalities and activities are integrated within a single entity. This model has defined the behaviour of buyers, sellers, platforms, and other stakeholders in the e-commerce value chain. However, it has limited the influence and participation of small businesses and offered limited choices for consumers.

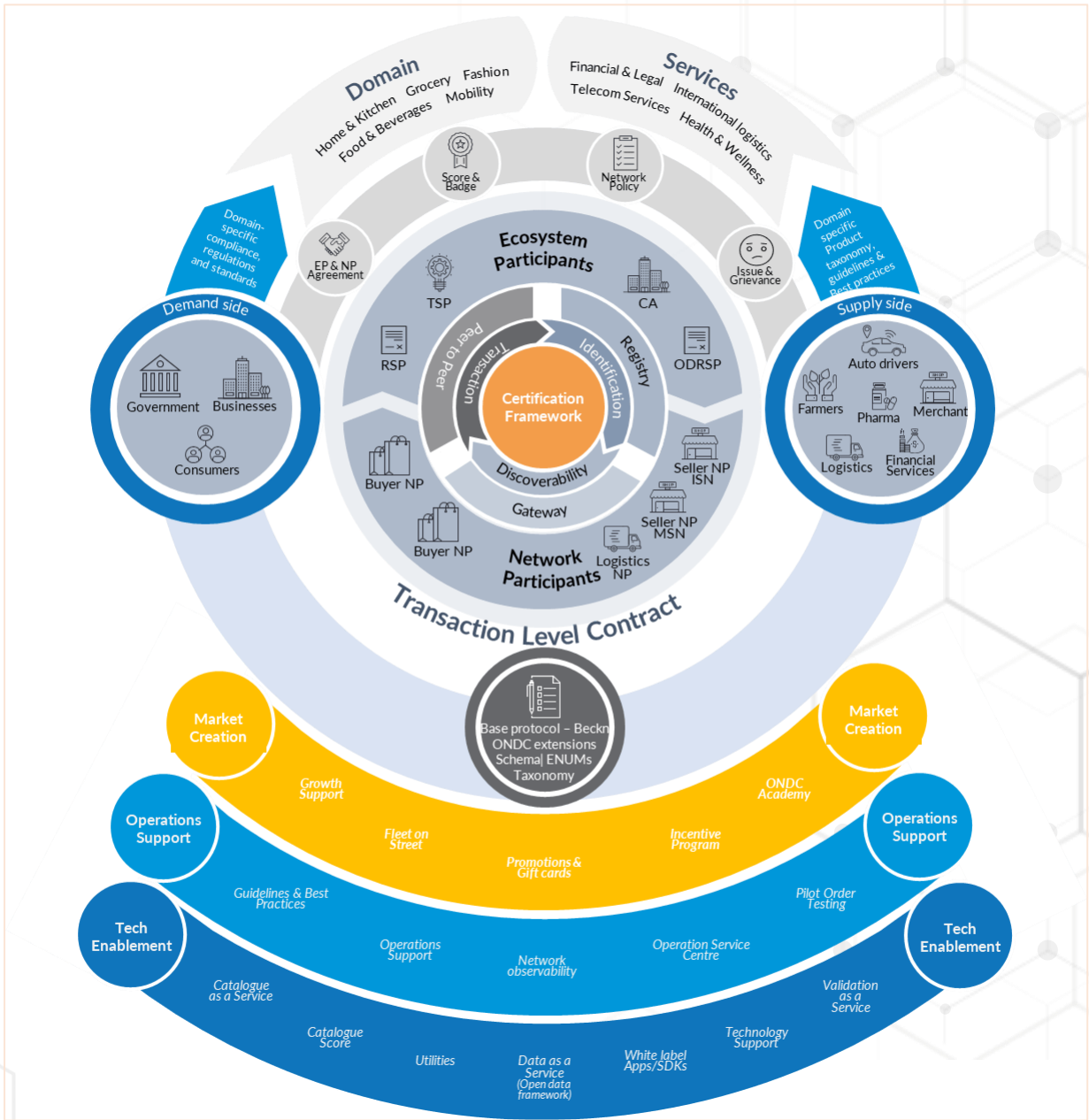
ONDC seeks to change this by introducing a decentralized model that breaks down the value chain into granular activities, a concept referred to as "unbundling." In this approach, different entities can handle various functions of an e-commerce transaction, allowing for a more distributed and inclusive ecosystem. ONDC's role is to provide an interoperable framework that enables seamless communication and collaboration among these different entities. By promoting interoperability, ONDC aims to foster a healthy, fair, inclusive, and competitive ecosystem for the ultimate benefit of buyers and sellers.

The value proposition of ONDC lies in offering an alternative to the centralized platform-based approach and empowering small businesses to have a more significant say in the e-commerce landscape. By facilitating interoperability, ONDC aims to stimulate innovation, diversity, and competition, ultimately leading to improved services and choices for buyers and sellers.

Overall, ONDC aspires to revolutionize digital commerce by shifting from a centralized platform model to a decentralized and unbundled environment, providing opportunities for a more inclusive and competitive ecosystem.

The picture below depicts a view of the ONDC's network:

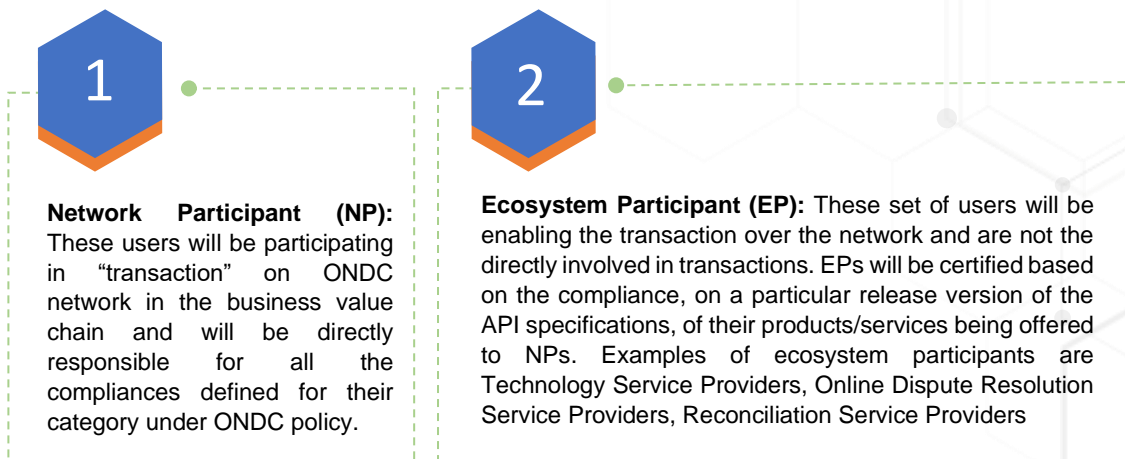
Figure 1: ONDC Big Picture



## 1.2 Participants in the ONDC network

ONDC has classified e-commerce participants into two categories based on their level of involvement as defined below:

Figure 2: Type of participants in ONDC network



Currently following e-commerce participants are identified within the ONDC network.

S. No	Participant Category	Name of Participants
1	Network Participant	Buyer Applications
2	Network Participant	Seller Applications which are of two types: <ul style="list-style-type: none"> <li>• Inventory Seller Nodes (ISN)</li> <li>• Marketplace Seller Nodes (MSN)</li> </ul>
3	Network Participant	Logistics Service Providers (LSPs)
4	Network Participant	Gateway
5	Ecosystem Participant	Technology Service Provider (TSP)
6	Ecosystem Participant	Reconciliation Service Provider (RSP)
7	Ecosystem Participant	Online Dispute Resolution Service Provider (ODRSP)
8	Ecosystem Participant	Certification Agency (CA)

**Buyer Applications:** Connects buyers to the ONDC network via a buyer application and shoulders buyer-facing responsibilities such as customer support, ensuring a seamless shopping experience, and providing a single checkout experience across categories.

Any business with a strong customer base can join ONDC as a buyer network participant. This can be through your existing application, a white-labelled app, voice assistant, chatbot, or any interface which can integrate with the network, and fulfil the feature requirements mentioned below. Buyer network participants can also choose to partner with a technology provider to create a buyer-facing interface integrated with ONDC.

Eligible buyer applications must fulfil the following feature requirements on their platform:

- Parse buyer search requests into relevant fields and searches the network for qualifying products on the network that fully/partially meet the search request.
- Display search results following the identifying criteria (closest store, product category, etc.).
- Display data aggregated from the network, such as rating, catalogue information (features, FAQ, specifications).
- Allow the buyer to add to the cart from multiple sellers/seller apps.
- Allow the buyer to select delivery options if more than one exists for the chosen seller/seller app.
- Check out (and pay) to initiate a purchase.
- Confirm the order with the seller app/seller and send confirmation to the buyer with the order ID.
- Allow buyers to reach out for any possible after sales support once a transaction has been completed using order ID.

**Seller Applications:** A Seller Network Participant is responsible for connecting sellers to the ONDC network through a seller application. They are also responsible for digitizing the seller's catalogue and dispersing payments. Additionally, they must train sellers on best practices in e-commerce to ensure quality fulfilment and provide a positive buying experience for customers.

- A Marketplace Seller Node (MSN) does not produce or manufacture any inventory of its own. It acts as a marketplace to offer goods and services that are provided by sellers.



- Inventory Seller Node (ISN) is any application operated by a seller who produces or manufactures and sells its own inventory. It doesn't include products/services by other sellers.

An interested Seller Node who intends to join ONDC network must provide following functionalities on their platform:

- Process buyer app search requests and share response based on the registered “available” seller’s product catalogues from correct category.
- Correctly check seller’s availability, display product’s T&Cs like return policy, refund policy defined by seller and share the same in response to buyer app.
- Provide delivery options and price to buyer app for the product based on the delivery address.
- Acknowledge the order confirmation from buyer app and share order id for tracking the request and any subsequent after sales requests.

**Gateway:** Gateways are essential components in an open-network ecosystem, serving as technology providers to ensure that all sellers in the ONDC Network can be discovered. They facilitate multicasting by forwarding search requests from buyer applications to all seller applications and vice versa, as specified in the ONDC Network Policies. The Gateway service enables manual searches by end consumers by providing relevant product/service information from ONDC's seller universe by verifying the request source from ONDC participant registry. Gateway lets you connect seamlessly, increase the reach & visibility and get relevant product/service information.

**Technology Service Providers (TSPs):** TSPs are crucial in offering a range of software applications either as standalone solutions or via cloud-based services. As an outsourced software provider, TSPs enable seamless business operations on the network, empowering players to participate in e-commerce without requiring in-house technology capabilities. TSPs also serve as drivers for achieving ONDC goals and attracting businesses of various sizes to join the network. TSP lets streamline your business operations, slash in-house tech hassles and scale & succeed effectively.

**Reconciliation Service Provider (RSP):** Reconciliation service providers are either ecosystem participants or functions within an NP, that receives the reconciled payment advice from a collector (NP that shall be collecting an amount to be settled to another NP) and initiates the transfer of funds between the NPs through a settlement agency. They help in handling fund settlement across NPs as per the terms and conditions agreed between these entities during the order placement journey.

**Online Dispute Resolution Service Provider (ODRSP):** Online Dispute Resolution (ODR) is the active use of digital frameworks to help resolve disputes between parties. ODR Service Providers (ODR SP), via dispute resolution methods such as mediation/ conciliation and/or arbitration, will attempt to resolve disputes between parties opting in the process of dispute resolution leveraging the services of these ODRSPs.

## 1.2.1 User journeys in the ONDC network

The below diagram depicts two user journeys in the ONDC network which are different from the ones from the user journeys in the platform.

Figure 3: Unbundled responsibility of **search & discovery** on the ONDC network

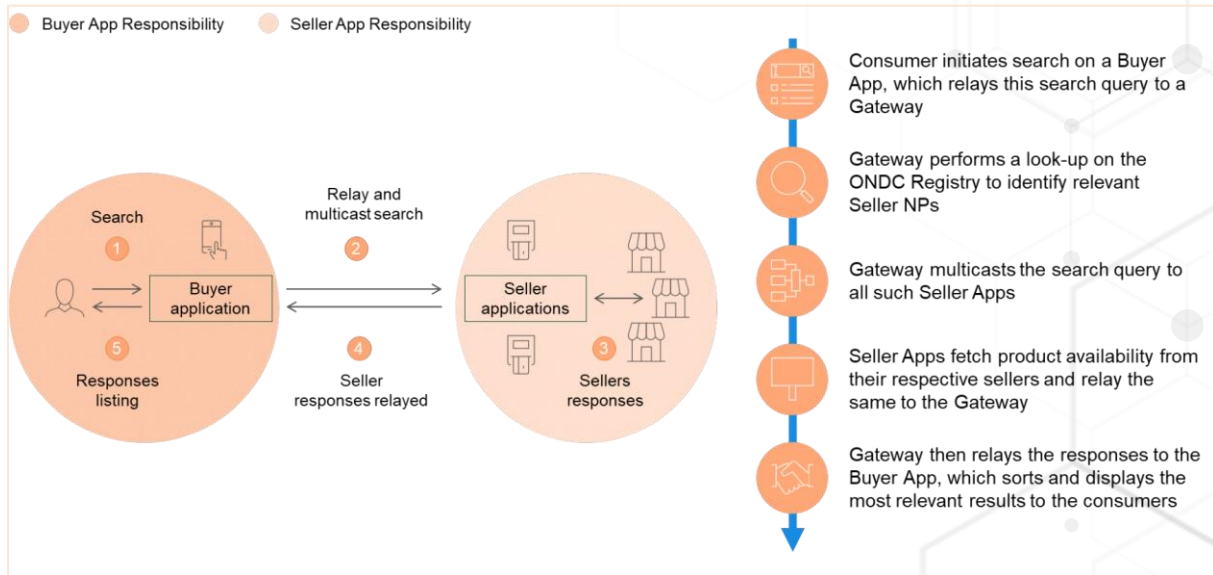
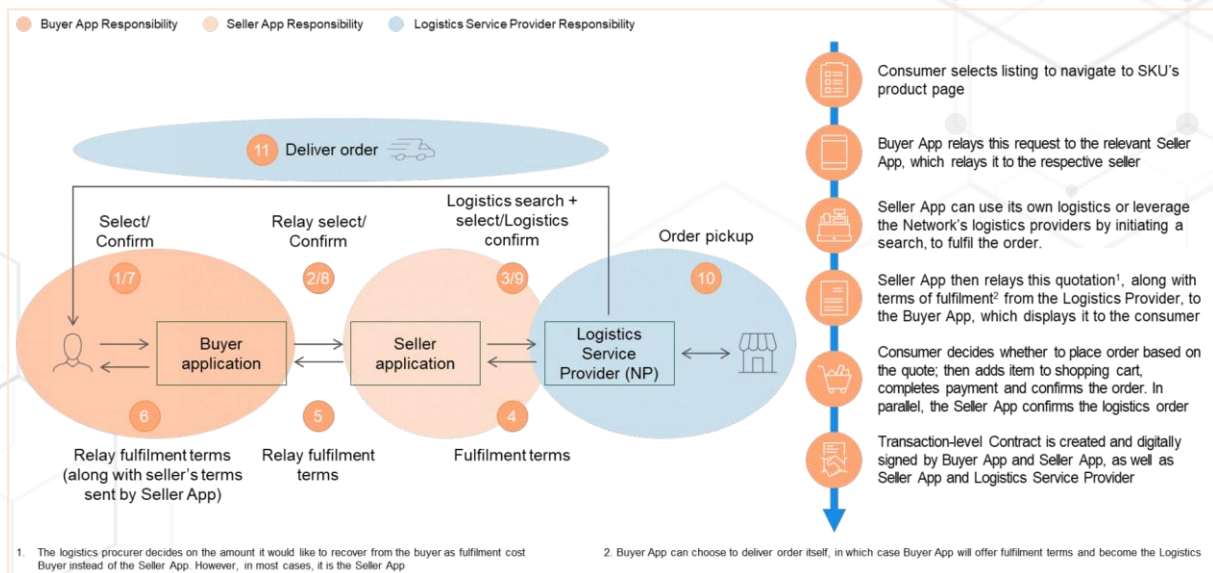


Figure 4: Unbundled responsibility of **ordering & fulfilment** on the ONDC network

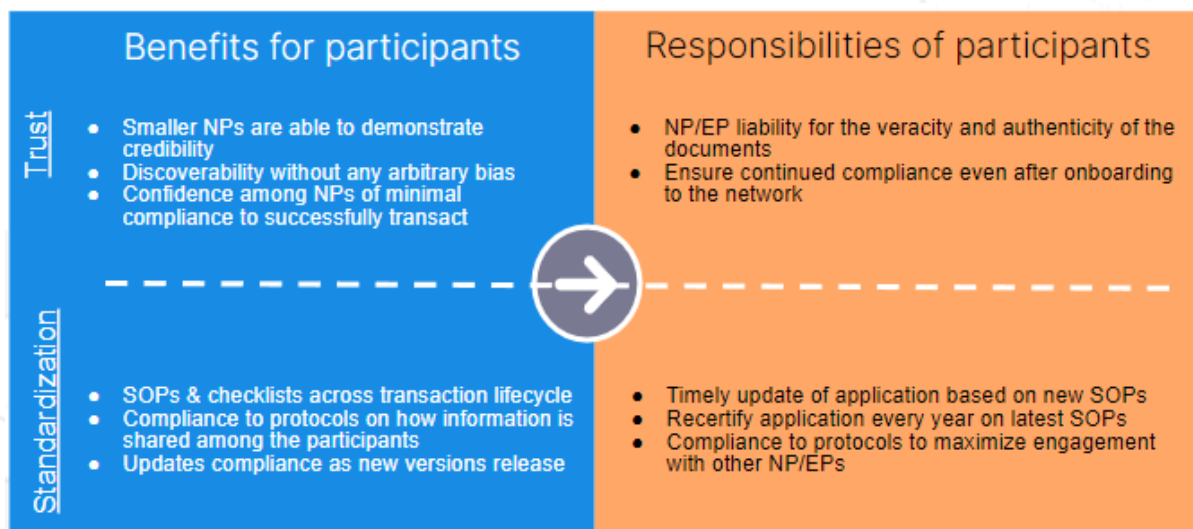


## 2 Certification Framework

The purpose of certification is to establish NP/EP's compliance to the various ONDC network policies requirements to participate in the ONDC Network and enable smooth onboarding and operations on the ONDC network. Certification framework will lay the foundation of trust in transactions on the ONDC network which would enable the network to grow and expand its footprint in fair and transparent manner. The certification framework will be enabled by onboarding a group of entities called Certifying Agencies whose roles and responsibilities are described in detail in following section. The trust will be built by the certifying agencies by ensuring that all onboarded participants have the necessary capacity and ability to carry out their designated role. The certification framework ensures that all parties within the ecosystem meet a certain standard of quality and security, thereby establishing a reliable and secure environment for transactions and interactions to build trust among NP/EP within the ecosystem. The certification will ensure that incoming participants possess the functional capabilities and ONDC network policies compliance requirements necessary to participate effectively in the network. Certification process will be carried out based on the pre-defined parameters detailed in the next section. Certification Framework will help in enabling trust-based environment and a seamless customer experience across search and discovery, order placement and fulfilment, payments and reconciliation and returns and customer grievances

However, the **certification framework does not aim to indicate the quality or reliability of services** offered by network participants.

Figure 5: Benefits to the participants and responsibilities of the participants to enable certification framework



### 2.1 Guiding Principles

The guiding principles of the certification framework have been designed to ensure **“Ease of Compliance”** and encourage participants of all sizes including nascent startups to become a part of the ONDC journey and succeed.



### Participant Centricity

In any network, it is essential that all participants have access to the necessary information and understand the requirements of the certification framework. By doing so, they can ensure that they are fully compliant with all necessary criteria before engaging with any certification agency. Having this level of transparency and accessibility helps to eliminate information asymmetry and promotes fair transactions between all parties involved. It allows for a level playing field where all participants are aware of what is expected of them and can make informed decisions accordingly. Ultimately, this creates a more efficient and effective network where participants can feel confident in their compliance with regulations and standards, while certification agencies can trust that they are working with informed and prepared network and ecosystem participant.

---



### SMART

The parameters for evaluation must be SMART (Specific, Measurable, Attainable, Relevant and Time-Bound) to enable an objective evaluation of participants on the ONDC network. The parameters should allow for the automation of certain evaluation processes which will evolve and add efficiency to the certification process.

---



### Generate Trust

The certification framework seeks to build trust amongst the network participants. Before starting operations on the network, it is important to assess a participant's capability to fulfil their role on the network.


---



### Adaptable

The certification framework should be adaptable to the future policy changes emanating from both regulatory and ONDC network policies. The e-commerce ecosystem across the world is continuously evolving and to cater to the needs of a dynamic sector, policies are likely to keep changing. Framework should also adapt to NP/EP diversity based on business maturity.

---



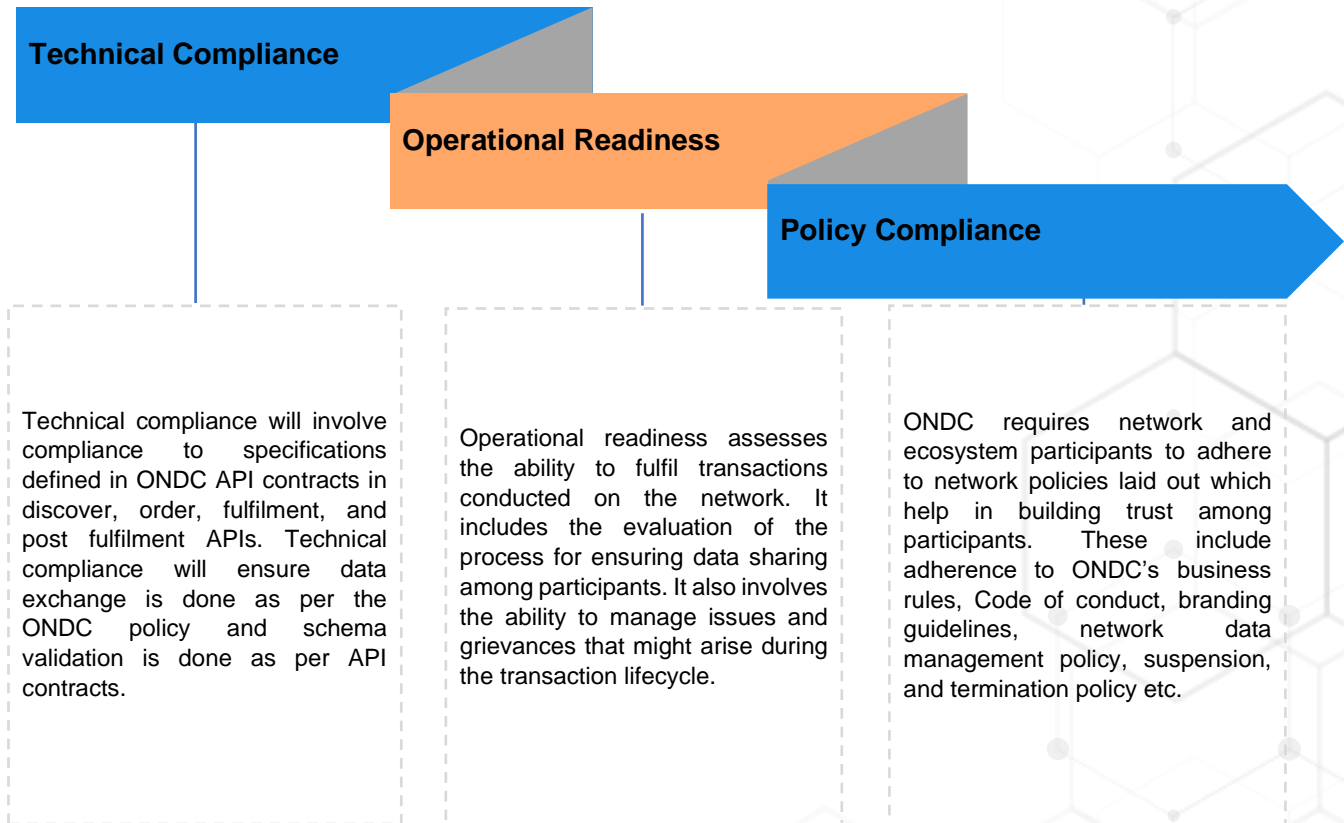
### Streamlined Mechanism

The certification framework is designed to follow a streamlined process for both implementations and evolution with future changes in technical compliance, operational readiness and policy compliance. The associated processes allow for periodic updates in a structured manner that allows for transparency and access to updates for ready reference for all NP/EP to ensure compliance to the requirements of ONDC network.

Given these guiding principles, the certification process will assess network participants and ecosystem participants through three lenses of evaluation which are described below.




























## 2.2 Lenses of Evaluation

The lenses of evaluation cover key aspects of the evaluation for network and ecosystem participants. Based upon each lens of evaluation, respective parameters and checklists have been defined which are the evaluation criteria to be considered by the certification agency while certifying a NP or EP in the ONDC network.



A NP who is being onboarded via TSP would be evaluated for operational readiness and policy compliance. However, such a NP who is onboarded via a Technology Service Provider (TSP) will be exempted from technical compliance as the technical compliance requirements would need to be fulfilled by the corresponding TSP.

Below table details out the evaluation requirement for all types of participants across the 3 lenses of evaluation.

S. No.	ONDC Participants	Participant Type	Technical Compliance	Operational Readiness	Policy Compliance
1	Buyer Applications	Network Participant			
2	Seller Applications (MSN and ISN)	Network Participant			
3	Logistics Service Providers (LSPs)	Network Participant			
4	Technology Service Providers (TSPs)	Ecosystem Participant			
5	Reconciliation Service Providers (RSPs)	Ecosystem Participant			
6	Buyer Applications via TSP	Network Participant			
7	Seller Applications (ISN and MSN) via TSP	Network Participant			
8	Logistics Service Providers via TSP	Network Participant			
9	Gateway	Network Participant			

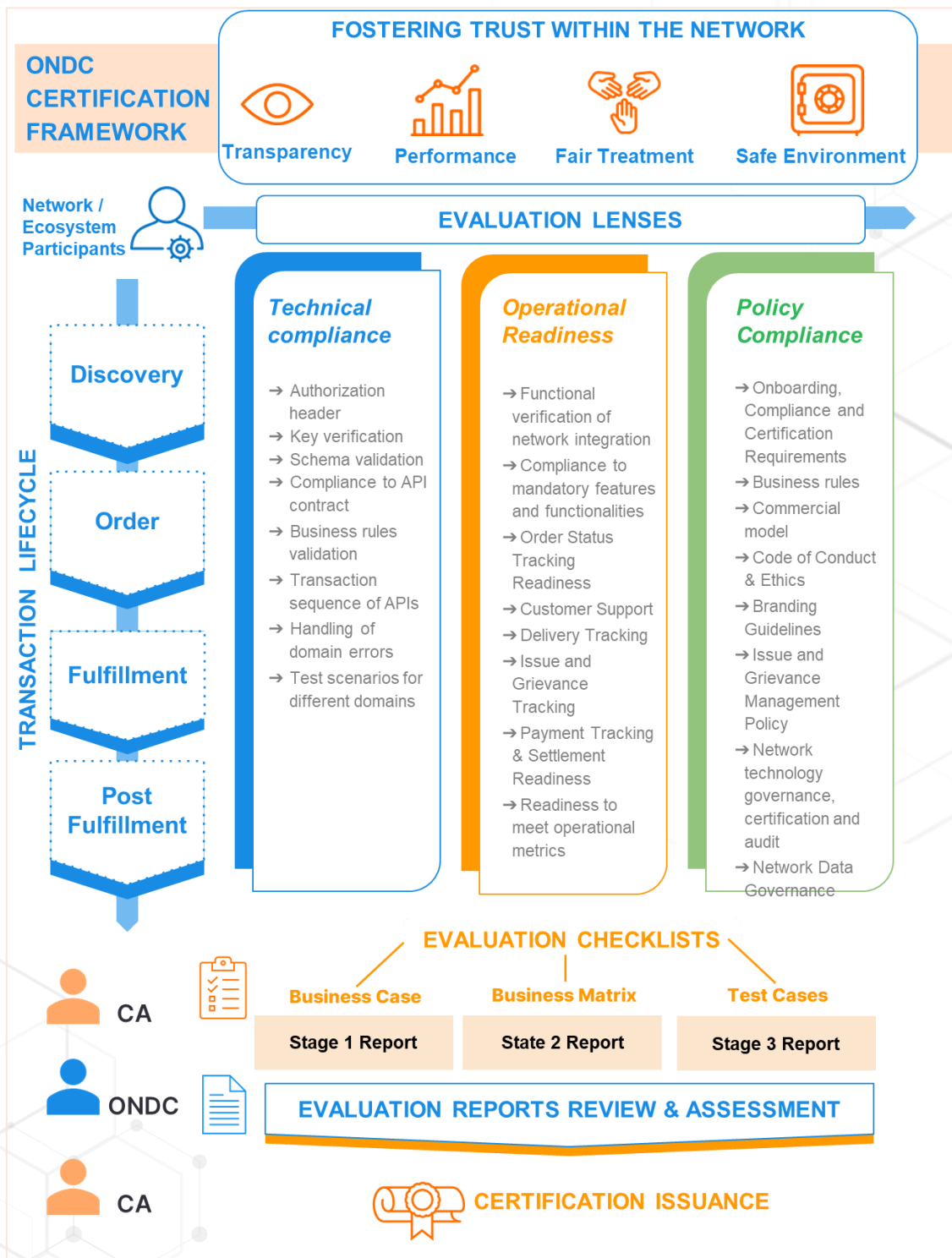
**Compliance Required**  **Limited Compliance** 

Breakups for role wise **Limited Compliance** are detailed in [Annexure 3](#).

## 2.3 Building Blocks of Certification Framework

Certification framework has been derived by leveraging ONDC's paper on "Building trust in the ONDC network" and ONDC's strategy paper with standard SOPs and checklists as depicted in the diagram below.

Figure 6: Building blocks of certification framework



The certification process is structured based on a set of checklists that outline the step-by-step flow of activities required for assessing an NP or EP by the Certification Agency (“CA”). These checklists are designed in accordance with the guiding principles outlined in the previous sections and they build upon each other to create a systematic approach to the certification process. The following sections provide a description of these building blocks.

### a. Define Lenses of Evaluation

Based on NP/EP role, the applicable lenses and relevant checklists for evaluation will be ascertained. For example, a buyer application getting onboarded on the ONDC network on its own would need to go through a complete checklist than a buyer application getting onboarded via TSP as the certain technical compliance would already have been fulfilled by a TSP. Key areas of evaluation for such buyer applications will be:

- **Technical compliance**

Technical compliance is an essential aspect of implementing the ONDC API contracts in the discover, order, fulfilment, and post-fulfilment APIs. It involves adhering to the specifications and guidelines outlined in these contracts to ensure proper data exchange and schema validation according to the ONDC policy.

Here's a breakdown of what technical compliance entails in the context of ONDC API contracts:

- Adherence to Specifications: Technical compliance requires implementing the APIs according to the specifications provided in the ONDC API contracts. These specifications define the required endpoints, request/response formats, authentication mechanisms, error handling, and other relevant details for each API.
- Data Exchange: Technical compliance ensures that data exchange between NPs/EPs complies with the ONDC policy. This involves transmitting and receiving data in the specified formats, such as JSON, and following the defined data structures and field validations outlined in the API contracts.
- Schema Validation: Schema validation plays a crucial role in technical compliance. It involves validating the structure and integrity of the data exchanged through the APIs. By validating against the API contracts' schemas, the implementation can ensure that the data conforms to the expected format and follows the defined rules and constraints.

By ensuring technical compliance to the ONDC API contracts, organizations can achieve standardized and reliable data exchange in the digital commerce ecosystem. This compliance helps promote interoperability among different systems and enables seamless integration and communication within the ONDC framework.

- **Operational readiness**

Operational readiness is a crucial aspect of the ONDC framework as it assesses an organization's ability to fulfil transactions conducted on the network. It encompasses various elements that ensure smooth and efficient transaction processing. Two key components of operational readiness are:

- KPIs: Operational readiness evaluates the process to ensure that participants can effectively execute transactions. It ensures that the NPs are able to achieve the key



operational KPIs set forth by the network such as fill rate, reconciliation and payment among others.

- Issue and Grievance Management: Operational readiness also involves the ability to manage issues and grievances that might arise during the transaction lifecycle. This includes establishing appropriate processes and mechanisms for participants to raise concerns, report problems, and resolve disputes. It encompasses tracking, escalation, and resolution procedures to address any issues efficiently and ensure a satisfactory experience for all participants involved in the transaction.

By evaluating and ensuring operational readiness, organizations can minimize disruptions, errors, and conflicts during the transaction process. It enables a smoother and more reliable flow of transactions within the ONDC network, enhancing trust and confidence among participants. Additionally, effective issue and grievance management processes help maintain healthy business relationships and facilitate prompt resolution of disputes, if they occur.

Overall, operational readiness is a critical factor in the successful implementation of the ONDC framework, as it ensures the efficient fulfilment of transactions and the effective management of any issues that may arise during the transaction lifecycle.

- **Policy compliance**

The framework establishes certain policies that participants in the network and ecosystem are required to adhere to. These policies are designed to foster trust, standardization, and consistency among the participants. Here are some of the key policies within the ONDC framework:

- Business Rules: The business rules set out the guidelines and regulations for conducting business transactions within the ONDC network. These rules outline the processes, procedures, and standards that participants need to follow to ensure fair and transparent interactions.
- Code of Conduct: The Code of Conduct defines the ethical and professional behavior expected from participants in the ONDC ecosystem. It outlines the principles of integrity, honesty, confidentiality, and compliance with applicable laws and regulations. Adhering to the Code of Conduct helps maintain a positive and trustworthy environment within the network.
- Branding Guidelines: The branding guidelines provide participants with instructions on how to use the ONDC brand and associated logos, trademarks, and visual assets. Adhering to these guidelines ensures consistent branding across the network and helps establish a recognizable and unified identity for ONDC.
- Network Data Management Policy: The network data management policy defines the guidelines and protocols for handling and managing data within the ONDC network. It includes aspects such as data privacy, security, consent, storage, sharing, and data lifecycle management. This policy helps protect the privacy and integrity of data exchanged within the network.
- Suspension and Termination Policy: The suspension and termination policy outlines the circumstances under which a participant's access to the ONDC network may be suspended or terminated. This policy ensures that non-compliance with the established rules and policies can lead to appropriate consequences, promoting accountability and maintaining the integrity of the network.

Adhering to these policies is crucial for participants in the ONDC network as it establishes a common framework for operating and collaborating. By following the network policies, participants can build trust, ensure consistent and reliable interactions, and foster a healthy and secure digital commerce ecosystem.

More details of these evaluation parameters can be viewed at [Annexure – Reference Links](#) section.

### b. Agree on Objectives

Given the lenses of evaluation, the area and objectives of the evaluation will be derived. These “objectives” of the evaluation will include the creation of verification mechanisms that will help in defining the business scenarios for checks during certification.

S. No.	Area	Objectives	Checklist
1	ONDC Policies	Ensure that participant comply to network policies that are established rules of the game while transacting on the network and set a level playing field for all network and ecosystem participants	<a href="#">Annexure 4.1</a>
2	Technical: Discovery	Ensure ONDC search API has been implemented correctly by NPs.	<a href="#">Annexure 4.2</a>
3	Technical: Order	Ensure information exchanged like inventory, prices and terms of payments are shown and communicated transparently across all NPs participating in the transaction.	
4	Technical: Fulfilment	Ensure end buyer and seller can view and share details related to product delivery and payment settlement between NPs in a timely and accurate manner.	
5	Technical: Post Fulfilment	Ensure NPs can rate overall experience of the transaction and seek support from the participant in case of an issue.	
6	Operations	Ensure that efficient information exchange is happening between sales and after sales support teams using an issue tracking tool and effective alert system. Data needed to prepare dashboard requirements are shared by NPs to ensure go-live operational readiness of NP/EP	<a href="#">Annexure 4.2</a>

### c. Define Scenarios

Based on the agreed-upon objectives, scenarios will be identified, against which a checklist will be developed. The scenarios should cover all the functionalities for each NP/EP. These

scenarios must be covered by CA, while checking compliance during the certification process. Detailed list of scenarios can be viewed in [Annexure 2 - Business Case Scenarios](#).

#### d. Define Checklists and Test Cases

Checklists with specific parameters needed to identify scenarios are developed for each type of NP/EP, based on the provided scenario statements. These checklists will be used by the certification agency during the evaluation process. The certification agency may include additional parameters for evaluation to the checklists based on the ones outlined in [Annexure - 3 Reference Test Cases](#).

#### e. Assess and Certify

The certification agency will assess each participant's application using the relevant checklists. If the participant satisfies the requirements outlined in the checklists, they will be granted certification. However, it is important to note that the certificate's validity is subject to recertification as detailed in the [recertification section](#).

## 2.4 Levels of Compliance in Certification Framework

### 2.4.1 Need for Levels of Compliance

To balance out the effort required during certification based on company entity and available features within the app, compliance levels based on business needs have been introduced. Levels of Compliance criteria defines the parameters based on which CAs can evaluate “cost of doing business” while engaging NP/EP for certification. The cost considerations may vary based on factors such as the type of operations and customer base, and can be negotiated between the NP and CA.

**Note: The compliance levels assigned to network participants will not be made public through any API requests or through the ONDC registry. However, NPs on their own discretion can mention their respective Level of Compliance on their website or application. Levels of Compliance will not be applicable for EPs. EPs will either be empanelled or whitelisted post qualifying the applicable requirements.**

### 2.4.2 Levels of Compliance Parameters

The approach for creating levels of compliance is based on the business characteristics of an application such as the number of successful transactions. Below table details out the parameters and rationale for selecting these levels of compliance:

S. No.	Parameters	Rationale
1	Number of Successful Transactions	Based on the expected number of transactions per month in conjunction with the e-commerce category helps in understanding expected load of number of searches and after sales queries.
2	Average Order Value	Average amount of the successful transactions NP is expected to perform on the network will help in understanding payment reconciliation & settlement process checks during certification.

Based on the parameters defined above, following Levels of Compliance have been identified for NPs:

1. Small Order scale compliance - focus is on certification compliance requirements keeping upcoming e-commerce players or participants who are expecting a lesser number of transactions and lower average order value.
2. Large Order scale compliance - focus is on additional requirements that must be met by mature organizations to maintain trust within NPs.

The correct level of compliance can be determined based on below parameters in the table given below.

Parameters	Small Order Scale Compliance	Large Order Scale Compliance
Number of Successful Transactions	Less than or equal to 2,000 / Month	Greater than 2,000 / Month
Average Order Value	Less than or equal to INR 500/-	Greater than INR 500/-

In case a participant crosses any of the thresholds for any parameter, the participant shall have to opt for the higher level of compliance for certification. Refer [Section 2.4.3](#) for an illustrative example that shows how this will manifest when evaluating which level of compliance applies to which NP.

While evaluating NP/EP certification requests CAs need to ascertain the functionalities required that need to be checked for compliance and create the final evaluation test pack for the certification process. Below are some of the reference parameters that can impact the test cases checklist to be executed.

S. No.	Parameters	Description
1	Product Category	Helps in identifying business domain(s) in which NP is operating and will help identify checks related to: <ol style="list-style-type: none"> <li>1. Product Taxonomy</li> <li>2. Domain specific policy compliance</li> </ol> <a href="#">Link to Existing Product Categories</a>
2	Payment Method	Based on the number of payment methods implemented by NP, CA will have to assess how many test cases will have to be executed.
3	Aggregation Capability	CA effort to validate business rules will increase considerably to ensure that aggregation from multiple sources has been done in compliance with ONDC policies compared to a single supplier NP.
4	Serviceability	Based on the serviceability of operations, CA will be able to evaluate other parameters like number of transactions in the right context.
5	Sales Channel	Based on the number of sales channels (B2C/B2B) compliance to different APIs need to be checked.

More parameters can be added by CAs while defining the final evaluation test pack for NP to determine the overall effort required for completing the certification process.

### 2.4.3 Illustrative Example

Below is the example of ABC limited, which approached Certification Agency for obtaining the certification to get onboarded on ONDC network.

Parameters	Parameter Value	Recommended Level
Number of Successful Transactions	1900 Transactions / Month	Small Order Scale Compliance
Average order value of the transaction	450/- per order	Small Order Scale Compliance

Although ABC Limited has qualified for Small Order Scale Compliance in terms of the number of successful transactions and average order value, ABC Limited can still opt for Large Scale Order Compliance certification depending on their future projections and business requirements.

## 2.5 Certification Process

The certification process can be envisaged as a 5-step process, which begins with the certification request and culminates in a final certification which is granted by a certification agency. All steps are mandatory for a certificate to be granted to a participant on the ONDC network. Below table describes the steps in detail:

Step	Initiated By	Description
Certification Request	Network Participant/ Ecosystem Participant	<p>The certification process begins with a certification request from a network participant <b>expressing their intention to start operating on the ONDC network</b>. Below is an illustrative list that is a part of a certification request that CA can request while understanding NP requirements.</p> <ul style="list-style-type: none"> <li>• Number of Successful Transactions - Based on the number of transactions in conjunction with e-commerce category helps in understanding expected load of number of searches, after sales queries based on which application should be checked.</li> <li>• Product Category - Helps in identifying the product taxonomy to be implemented and effort that would be required to verify the same</li> <li>• Average Order Value - Helps in identifying the expected value of the transaction.</li> <li>• Registration Details: Basic details about the company which can help CA verify company identity.</li> <li>• NP Type – One of the predefined NP that has been defined in above <a href="#">section 1.2</a></li> <li>• Point of Contact – Contact person who will be leading the certification activity on NPs behalf</li> <li>• Platform URL – URL/App details that will be joining ONDC network</li> <li>• Sales Channels – Channels through which NPs will be doing transactions. Possible values for these are: <ul style="list-style-type: none"> <li>○ B2C – Website</li> <li>○ B2C – Mobile</li> <li>○ B2B – Website</li> <li>○ B2B – Mobile</li> </ul> </li> <li>• Serviceability – Geolocation (s) where NP will be operating like States, Cities or Across India</li> <li>• Requested Level of Compliance – Compliance level in which NP wishes to be certified based on its expected transaction volume and the same will be assessed by CA.</li> </ul> <p>Once the requirements are finalised, the certification agency initiates the certification process by evaluating the NP/EP for stage 1 evaluation.</p>

Step	Initiated By	Description
Stage Report 1	Certification Agency	<p>The Stage 1 Report <b>outlines the compliance checks for onboarding NPs from Staging to Pre-Production<sup>1</sup></b>. The Stage 1 Report outlines metrics around the list of services offered by a participant on the network. The following aspects are checked in the Stage 1 Report along with the checks defined in stage 1 checks.</p> <ul style="list-style-type: none"> <li>• Onboarding Directly or through TSP (Yes/No)</li> <li>• API versions of transaction</li> </ul>
Stage Report 2	Certification Agency	<p>The Stage 2 report by <b>Certifying Agency (CA) requesting ONDC to initiate onboarding of NP on production</b> for the probation period. The following additional artefacts are generated at Stage 2</p> <ul style="list-style-type: none"> <li>• Executed result sheet for stage 2</li> <li>• Addon services required (e.g., VAPT, App scan)</li> <li>• Period of Probation</li> <li>• Operations readiness dashboard</li> </ul>
Stage Report 3	Certification Agency	<p>Stage 3 report is created by the Certifying Agency (CA) <b>after the completion of the probation period, requesting either to extend the probation period or confirm certification completion</b> based on the NP during the probation period. The following artefacts are created during the probation period.</p> <ul style="list-style-type: none"> <li>• Executed result sheet for stage 3</li> <li>• Status of other services offered</li> </ul>
Certificate	Certification Agency	<p><b>Final certificate by Certifying Agency (CA).</b> The certificate should be digitally verifiable. The Certificate provided by the Certification Agencies must contain the following information:</p> <ul style="list-style-type: none"> <li>• Certificate number with QR Code</li> <li>• Validity of certificate</li> <li>• Level of Compliance Granted</li> <li>• Recertification date</li> <li>• API Version number</li> <li>• List of EPs if applicable</li> <li>• Product Category</li> </ul> <p>If the certification agency finds that the participant has passed these tests up to the satisfaction of their defined processes, the certification will be issued to the Network participants. And will be submitted by Network Participant to ONDC.</p>

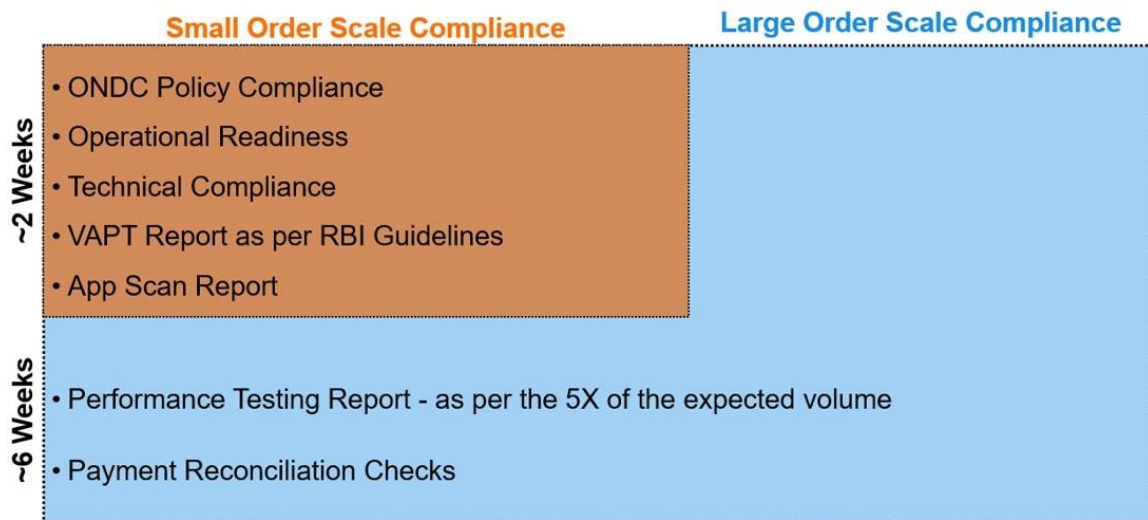
<sup>1</sup> Staging to Pre-Production denotes the NPs/EPs initial development and to start with the validation of developed applications with ONDC Reference Buyer/Seller Apps.

## 2.6 Timelines for Evaluation

The time required for the certification procedure may differ depending on the levels of compliance and the evaluation test pack derived from the final checklist based on business needs.

The below timelines are indicative in which CA should be attempting to complete the certification process. CAs are encouraged to automate the certification process to reduce these timelines. The timelines are also subject to the processes involved in the certification process. The journeys involved in the certification process are also subject to the participant type since different participants are required to comply with different compliance checks.

Figure 7: Requirements for different "levels of compliance"



**Note: The timelines are indicative and they will be updated on the basis of level of complexity and level of automation that CA can provide while certifying NP/EP.**



## 2.7 Different Journeys for Different Participants

The certification journey for different types of participants will vary depending on the type of network/ecosystem participants. Stage 3 report is not applicable for ecosystem participants as there will be no probation period for EPs.

Figure 8: Network Participant Journey

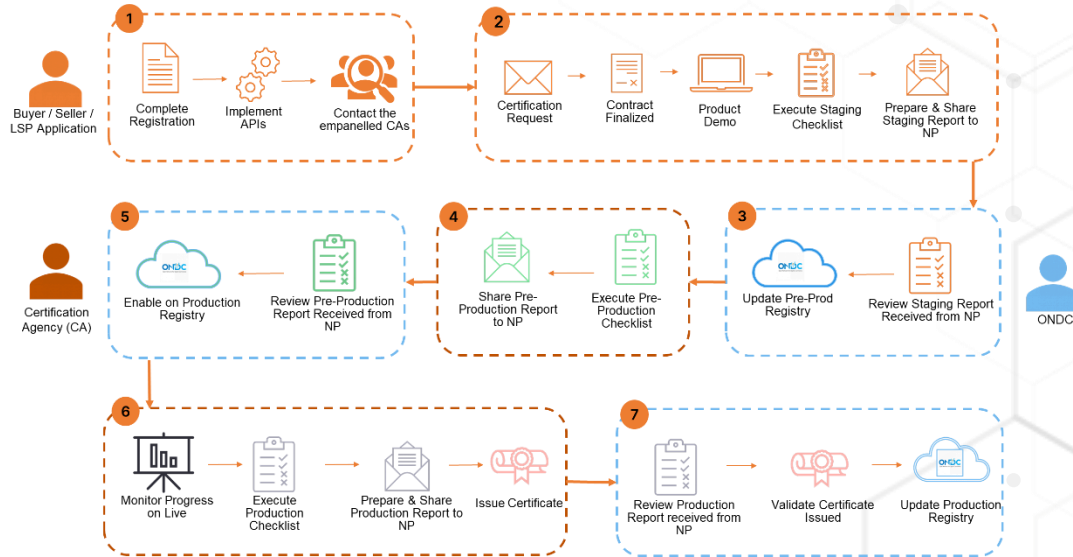
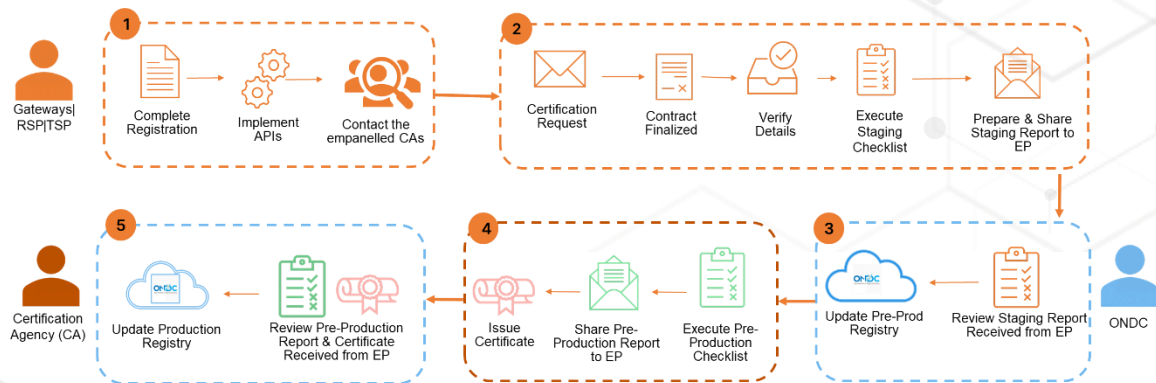


Figure 9: Ecosystem Participant Journey



### 2.7.1 ONDC Policy Compliance / KYC / Signed Undertaking (as per Law)

Policy compliance entails compliance with all policies related to e-commerce defined by ONDC, including basic KYC requirements. While some policy requirements are measurable and verifiable through a third-party certification agency, policy requirements which are intangible will be met through self-declarations and undertakings signed by participants as a part of the certification process requirements. Policy compliance checklist as mentioned in [Annexure 1](#) has to be prepared by CA based on the following laws based on the Network Participants sectors and nature of business:

- Consumer Protection Act, 2019
- Consumer Protection Act (E-Commerce) Rules, 2020
- Legal Metrology Act, 2009
- Information Technology Act, 2000
- Information Technology Rules (Intermediary Guidelines and Digital Media Ethics), 2011
- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
- FSSAI Act, 2006 (for F&B related NPs)
- Motor Vehicles Act (Logistics related services)
- Fair Packaging and Labelling Act Microbead-Free Waters Act of 2015 (Domain Specific)

Laws may get added to the above list based on the adoption of new categories or revision to the existing regulations.

## 2.8 Continuous Assessment and On Demand Recertification

To ensure continued network health of the ONDC network, participants must be continuously evaluated and ONDC should be able to demand recertification in case of any suspicious activity. To enable this, there is a provision of continuous assessment and on-demand recertifications in the certification framework.

### 2.8.1 Continuous Assessment

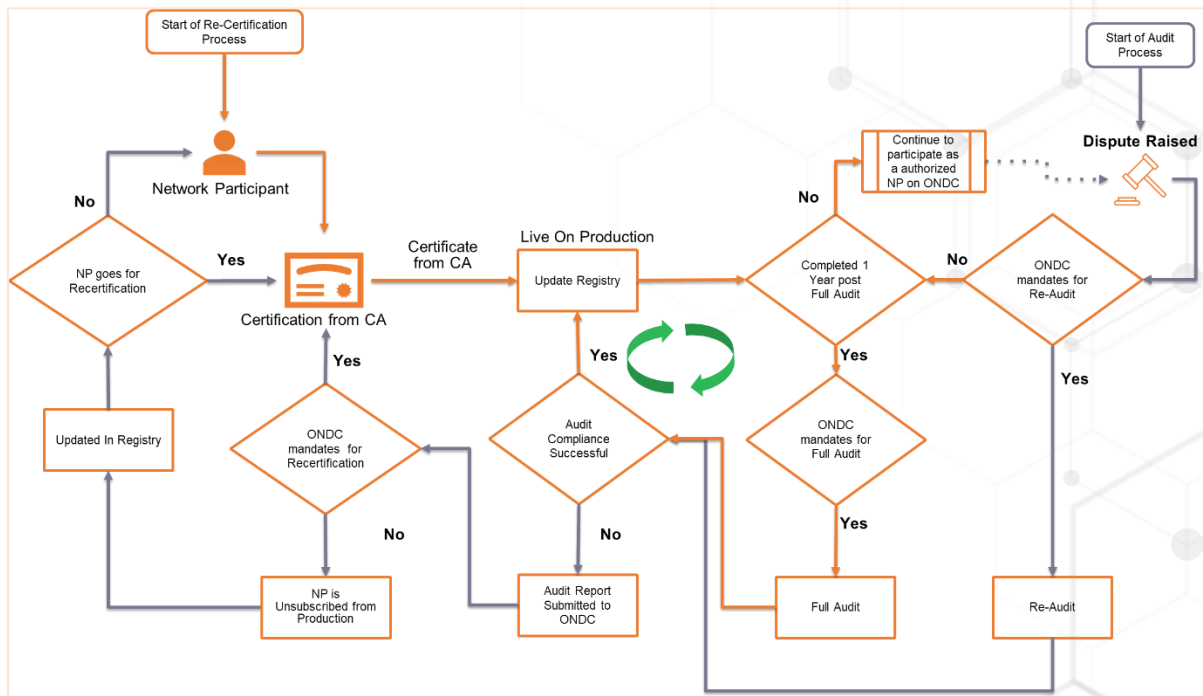
Participants may be re-evaluated on a periodic basis in compliance with the ONDC policies. These periodic audits would incentivize network participants to ensure compliance on a continuous basis to avoid a potential recertification request from ONDC, in case any non-compliant behaviour is noticed on the part of a participant. Participants will be incentivized to ensure compliance throughout the cycle to avoid any potential re-certification requests. Audits serve as a checkpoint for compliance and will be conducted in a timely manner. In the event of fraud, a forced audit will be conducted at the network participant's expense. To conduct an audit, ONDC will provide the participant with a list of requirements that must be followed. This ensures that the audit process is standardized and consistent across all participants.

#### 2.8.1.1 Triggers for Continuous Assessment

Below is the list of trigger events for continuous assessment:

- NPs/EPs have been notified of non-compliance against the network policies.
- NP/EP updates their solution e.g., re-architected the solution, changed TSP.
- The policy mandates for the initiation of recertification.

Figure 10: Continuous Evaluation and Re-Certification Workflow



➔ Fresh certification process

➔ On-Demand Recertification process

## 2.8.2 On-Demand Recertification

If ONDC detects suspicious activity on the network by a participant, the organization reserves the right to request that participant undergo recertification. The recertification process may involve a complete or partial evaluation, depending on the specific need for re-evaluation. The cost of recertification will be borne by the participant who is directed to undergo the process. Certification is the starting point for compliance when onboarding and using the ONDC network. Participants must be certified in order to use the network. Recertification is required in cases of non-compliance or when a new protocol version is released. This ensures that participants remain up to date with network standards and protocols.

### 2.8.2.1 Triggers for On-Demand Recertification

Below are the triggers for On-Demand Recertification process:

- To comply with the standards and protocols of the ONDC network, participants must first obtain certification before they can use it.
- Recertification is necessary in cases of non-compliance or when a new protocol version is released, in order to keep participants up to date with the network's standards and protocols.
- Recertification is a means of ensuring ongoing compliance and maintenance of network standards.
- If fraud is suspected, the network participant will be required to undergo recertification at their own cost.
- ONDC will furnish the participant with a set of guidelines to be followed in order to conduct the recertification process.
- It assures that the recertification procedure is uniform and equitable for all participants.

### 3 Roles & Responsibilities of Certification Agency

Currently, the ONDC team does in-house checks on the involved network participants using various aspects of compliance against the network policy. However, it may not suffice with the potential growth of the network.

As the network expands and the number of users increases, the empanelled certification agencies will take on the function of verifying network participants' capacity to function and conduct audits to ensure continued network health. To ensure that network participants have enough confidence to leverage the unique service offerings of other network participants, a certification agency needs to verify the capability of all network participants to offer their unique services.

In essence, the certification framework can be seen as the cornerstone of trust in transactions on the ONDC network which would enable the network to grow.

Certification Agencies (CAs) will issue digitally verifiable certificates to all network and ecosystem participants based on criteria such as type of network participant, policy compliance, operational capability, technical capabilities. Certification Agencies are the fulcrum of the entire certification process. Given that certification agencies will be the key driving force behind growth of the network, it is important to pre-define their roles and responsibilities to ensure that they fulfil all essential requirements of the certification process.

To ensure trust between NPs/EPs, certification framework has been envisaged by ONDC to drive the baseline capability requirements to reliably offer services to other network participants. Certification agencies are planned to be empanelled as an ecosystem participant to assist the network participant in their journey to become ONDC compliant. The CA would verify the compliance of the network participants against the certification framework. The certification agencies would also conduct audits at various life stages of the network participant to ensure continued network health. CAs will issue certificates to all network participants and ecosystem participants based on criteria such as type of participant, policy compliance, operational capability, technical capabilities etc.

These roles and responsibilities are described below.

- **Creation of Run Book:**

The certification agency will specify the evaluation processes of participants based on the evaluation requirements specified in the certification framework. While the checklists are provided as part of the certification framework for the reference of a certification agency, further refinements, additions and amendments, costs and time involved in verification is for the certification agency to decide and specify. CA is expected to create a runbook and submit it to ONDC for review and approval as a part of empanelment exercise.

Runbook will be prepared by the CA in a defined format to perform the certification process, based on the NP/EP details furnished.

Runbook should include:

Artifact	Description
Business scenarios	Reference list of business scenarios that they are expected to verify during the certification process. Reference business scenarios have been defined in section <a href="#">Annexure 2</a> . This list will be enhanced during the process of certification as the NPs

Artifact	Description
	will be providing the updates to the Scenarios as per their area of operations.
Business case matrix	Comprehensive list of business case matrix mapping it to the transaction lifecycle. Reference business matrix have been defined in section <a href="#">Annexure 2</a>
Test Cases	Comprehensive list of test packs that will be executed by CA during the certification process.
Sample Report Format	Standardized report format that would be shared by CA to ONDC has been added in the <a href="#">Annexures 4</a>
Certificate Sample	A sample copy of certificate that would be granted to NP/EP by CA as defined in <a href="#">Annexure 5</a> .

Runbooks created by CA are intellectual properties of CAs that have to meet the minimum compliance requirements. Each CA will have to submit a runbook created by them for review before the same can be used for evaluation.

- **Verify NP Details Authenticity:**

It would be the responsibility of the certification agency to verify the authenticity of the documents furnished by the participants. While the participants are required to provide authentic documents, it would be the responsibility of the certification agency to verify the veracity of the provided documents.

- **Evaluate NPs:**

Based on the CA's run book derived from the ONDC checklist added in [Annexures](#), the certification agency will undertake the evaluation of the participants and issue digitally verifiable certificates. Based on the certification issued, the participants will become eligible for participating on the ONDC network.

- **Share Assessment Reports based on Evaluation conducted:**

Based on the verification process undertaken by certification agencies, an assessment report would be required to be furnished from certification agencies to ONDC and NP/EP. The assessment report will add credibility and overall transparency to the certification process. In case, the assessment could not be completed successfully, participants can come back to the same CA for re-evaluation at a later date as per the mutually agreed timelines between NPs/EPs and CA.

- **Adherence to Timelines:**

The certification agencies would be required to publish results within a stipulated timeline agreed in contract between NPs/EPs and CA. While the certification agency is free to decide upon a timeline and communicate the same to participants, the breach of any communicated timeline may invite liquidated damages (the nature of penalties would be a part of the contract between participants and certification agencies, hence would be driven by market outcomes)

- **Issue Verifiable Certificates:**

Certification Agencies would be required to furnish digitally verifiable certificates which can be accessed and verified by ONDC as well as other participants on the ONDC network. Ease of access and verification would be necessary to ensure transparency and trust in the ONDC network.

- **Respond to Queries After Certification Process:**

Certification Agencies must deploy mechanisms to ensure that queries regarding the issued certificates and the involved processes are responded to within pre-stipulated timelines. Certification Agencies must ensure that personal sensitive data of clients (ONDC participants) is not revealed, and only general non-identifiable information is revealed while responding to such queries.

- **Revision and Revalidation of Runbook**

In order to keep pace with the changing protocols and new API contract defined by ONDC, certification agencies would be required to keep pace with the changes done by ONDC to ensure their certification guidelines are up to date. This will ensure that onboarded NPs can maintain the minimum compliance requirements as per latest protocol.

**Note: All CAs shall create and continuously improve automation capabilities to execute the checklists defined in runbook to reduce the time required for certification for faster onboarding of NPs on network.**

### 3.1 Runbook Update Process Steps

When releasing a new version of API protocol/s, ONDC will also publish the timelines for feedback and implementation of the same by NPs and EPs. CA would be required to update run books and automation capabilities as per the communicated timelines by ONDC. It is possible that during checklist update, if new scenarios are identified and should be the part of the minimum acceptance criteria, ONDC might re-publish the reference business cases or revised version/s of API protocols accommodating feedback received from CAs or NPs/EPs.

Once CAs are onboarded, ONDC will facilitate in defining a process along with the templates and timelines for updating the runbooks and test cases.

Figure 11: Process to build the runbook



## 3.2 Runbook Update Process example

Sample Runbook update triggers are explained below with the example:

### ➤ Test Pack Update Trigger

- Protocol Version Upgrades
  - Major version changes from v1.0.0 to v 2.0.0
  - Minor version changes from v1.0.0 to v1.1.0
- Taxonomy Updates
  - Addition of new taxonomy, ex. Electronics industry addition
  - Updates made to existing taxonomy based on version changes, ex. Fashion taxonomy sub-parameters changes for version upgrades
- Category updates
  - Addition of the Electronics industry to the categorization
  - Removal of Packaged Tin Food under Packaged Food category
- Levels of Compliance Redefinitions
  - Benchmarking added for return or refund of orders

### ➤ Runbook Updates & Submission to ONDC

- Runbook updates made
  - Business Case additions for the Electronics Industry or removal of category
  - Scenarios updates on the removal of Packaged Tin Food & changes made to taxonomy parameters
  - Test Cases added new for Electronics Industry
  - Test Cases modified for Packaged Food category for removal of Tin Food
  - Test Cases modified for version v2.0.0
  - Test Cases modified for version v1.1.0
  - Operational cases added by ONDC based on issues found in production
- Runbook updates & submission for review to ONDC
  - Certification Agency makes the necessary changes for Electronics Industry
  - Certification Agency removes the Packaged Tin Food test cases & scenarios in the Test Pack
  - Submission of the new Test Pack for review for the Travel Industry & Packaged Food

### ➤ Test Pack Validation by ONDC

- Run Book Validations
  - Test Pack validations for Electronics Industry & Packaged Food category changes
  - Test Pack validations for version changes
- Confirmation to Certification Agency on the latest validation



- Test Pack validation successful for Electronics Industry & Packaged Food
- Test Pack validation successful for version changes

**Feedback and suggestions on the certification framework:** Please share your suggestions or feedback on Certification Framework on the email ID [neeraj@ondc.org](mailto:neeraj@ondc.org) and [tech@ondc.org](mailto:tech@ondc.org) with the sub: "Certification Framework"

## 4 Annexures

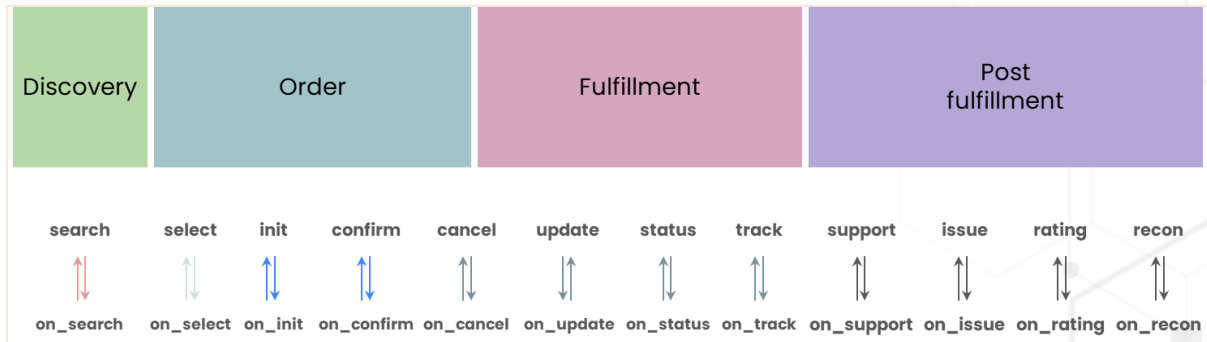
### 4.1 Annexure 1 – ONDC Policy Compliance Checklist

S. No.	Evaluation Criteria	Checklist	Verification	Declaration
1	KYC Documents	GSTIN Number	Yes	No
2	KYC Documents	Company declaration of authorized signatory to authorize contact person for registration process	No	Yes
3	KYC Documents	Registered Mobile No. of any of the authorized person	Yes	No
4	KYC Documents	Nodal Like Account (if collecting payments)	Yes	No
5	KYC Documents	TAN	Yes	No
6	Policy Requirements	Legal Entity Name	Yes	No
7	Policy Requirements	Business Address	Yes	No
8	Policy Requirements	Grievance Officer Number and Name	Yes	No
9	Policy Requirements	Signed soft copy of NP agreement	Yes	No
10	Policy Requirements	List of classification criteria for sorting catalogue of products (Testing for arbitrary classification for Buyer App only)	Yes	No

## 4.2 Annexure 2 – Business Case Scenarios based on APIs

List of reference business cases have been defined based on possible transaction workflows that happen during the transaction lifecycle. ONDC protocols divide the transaction lifecycle in following phases and APIs that are executed as a part of the process.

Figure 12: ONDC Key APIs



These business cases define the possible business centric combinations across these stages that need to be validated to ensure that NPs/EPs have completed the implementation of minimum features required to be onboarded on ONDC platform. Next section covers the business scenario and possible use cases to be checked at every stage to ensure successful execution of the business scenarios. CAs are also expected to know the key input parameters and expected outcome of API responses so the same can be validated during execution of business scenarios. Refer below link which lists out reference scenarios that can be used to create a comprehensive list of business scenarios for evaluation of NPs/EPs.

### [Reference Business Scenarios](#)

In order to create an automaton framework to test these business scenarios, CAs are encouraged to map these scenarios as a “Yes/No” matrix for key combinations of data points that influence the workflow of a transaction. Below points cover some of these data points for reference. CAs can add more into these to define a testing framework and can automate these by creating a sandbox environment that can be used by NPs during certification to reduce the time for verification. Below section details out the key attributes that can be used to define the automation test cases for faster verification to compliance:

- **Identifier** – Identification code for the selected business case scenario
- **Business Case Description** – Short description of the business case scenario outcome of the combinations defined in the grid.
- **Cancellable** – Product’s attribute provided by the respective seller, to define for the product cancellation will be allowed or not.
- **Returnable** - Product’s attribute provided by the respective seller, to define for the product return will be allowed or not.
- **Multiple Product Selection** – For the selected business case, the buyer will be selecting a single product for the journey or will be selecting multiple products for the journey.

- **Multiple Quantity Selection** – For the selected business case, the buyer will be selecting a single quantity for the journey or will be selecting multiple quantities for the journey, irrespective of a single product selection or multiple product selection.
- **Multiple Delivery Address** – Business case identified when the billing & delivery addresses will be different from each other during the business case journey.
- **POD (Payment On Delivery)** – Buyer selects with the payment process to be Cash on Delivery for the selected business journey, and the information to be provided to the seller fulfilling the request.
- **Pre-Paid** – Buyer performs the payment for the selected order, to proceed with the business case journey, for pre-paid orders.
- **Order Confirmed by Seller** – Seller on receiving the order details, can confirm or reject the order, based on serviceability & in-stock quantities of the product requested.
- **Pre-Dispatch Cancellation** – Business journey defined, as when the Buyer cancels the order being in the Pre-Dispatch stage, but not yet dispatched. A return order journey will be initiated for the current business scenario.
- **Partial Cancel Order** – The buyer is not having any requirement for the product or quantity any more, and has the option to partially cancel the order and go on with the delivery of the other scheduled products in the current order.
- **Full Cancel Order** – The buyer is not having any requirement of the current product & quantity, can proceed with the full cancellation of the order. Sellers if are not able to serve for the product or quantity can call for the full cancellation order.
- **Partial Return** – The buyer, if not satisfied with some of the product or quantity for the delivered order, is allowed to initiate the partial return of the order. And the information is shared with the seller as soon as the return is initiated.
- **Full Return** – The buyer is not satisfied with the complete delivered order, and can initiate the full return of the order.
- **Return Confirmed by the Seller** – For the products defined as returnable true, the return can be initiated by the buyer. For the return initiated, the seller receives the information & is allowed to confirm or reject the return order request.

### 4.3 Annexure 3 – Reference Test Cases based on NP/EP Type

S. No.	Name of the Document	Description of the document	Link
1.	Business Case Matrix	Business Case Matrix to help out with the automation scenarios	<a href="#">Link</a>
2.	Business Case Scenarios	Business Case Scenarios based on the APIs & parameters	<a href="#">Link</a>
3.	Certification Framework Test Cases for Buyer App	Detailed test cases for the Buyer App	<a href="#">Link</a>
4.	Certification Framework Test Cases for Buyer App via TSP	Detailed test cases for the Buyer App via Technology Service Provider	<a href="#">Link</a>
5.	Certification Framework Test Cases for Seller App	Detailed test cases for the Seller App	<a href="#">Link</a>
6.	Certification Framework Test Cases for Seller App via TSP	Detailed test cases for the Seller App via Technology Service Provider	<a href="#">Link</a>
7.	Certification Framework Test Cases for LSP	Detailed test cases for the Logistics Service Provider	<a href="#">Link</a>
8.	Certification Framework Test Cases for LSP via TSP	Detailed test cases for the Logistics Service Provider via Technology Service Provider	<a href="#">Link</a>
9.	Certification Framework Test Cases for TSP	Detailed test cases for the Technology Service Provider	<a href="#">Link</a>
10.	Certification Framework Test Cases for Gateway	Detailed test cases for the Gateway	<a href="#">Link</a>
11.	Certification Framework Test Cases for RSP	Detailed test cases for the Reconciliation Service Provider	<a href="#">Link</a>
12.	Certification Framework Test Cases for IGM	Detailed test cases for the IGM	<a href="#">Link</a>

#### 4.4 Annexure 4 - Assessment Report format

S. No.	Name of the Document	Description of the document	Link
1.	Assessment Report	Output Report as per ONDC guidelines	<a href="#">Link</a>

## 4.5 Annexure 5 - ONDC Certificate Data Points

Following data should be clearly visible on the certificate generated by the CA for the respective NP/EP.

S. No.	Name of the Parameter	Description of the Parameter
1.	Name of the Company	Company Details
2.	NP/EP Type	Type of Participant as defined in <a href="#">section 1.2</a>
3.	Category	From the list the available categories defined in ONDC protocols.
4.	Date of Issuance of Certificate	Date on which certificate is issued
5.	Validity of the Certificate	Duration or End date of the Certificate
6.	ONDC Protocol Version	Protocol Version on which Certificate was issued
7.	Authorised Signatory (from CA)	Digital Signature of the Certification Agency
8.	TSPs	Name of the TSP, if any

## 4.6 Reference Documents/Links

S. No.	Name	Category	Link
1.	ONDC GitHub	Technical	<a href="#">Link</a>
2.	ONDC Strategy Paper	General	<a href="#">Link</a>
3.	ONDC Business Briefing Presentation	General	<a href="#">Link</a>
4.	ONDC Business Briefing recording	General	<a href="#">Link</a>
5.	ONDC Tech Briefing Presentation	Technical	<a href="#">Link</a>
6.	ONDC: Tech QuickStart Guide	Technical	<a href="#">Link</a>
7.	ONDC Network Policy	Policy	<a href="#">Link</a>
8.	ONDC Integration Guide	Operations	<a href="#">Link</a>
9.	ONDC Retail API Contract v1.1.0	Technical	<a href="#">Link</a>
10.	ONDC Logistics API Contract v1.1.0	Technical	<a href="#">Link</a>
11.	ONDC RSP API Contract	Technical	<a href="#">Link</a>
12.	ONDC IGM API Contract	Technical	<a href="#">Link</a>
13.	ONDC Rating API Contract	Technical	<a href="#">Link</a>
14.	Existing Product Categories	Technical	<a href="#">Link</a>