Data Integration Platform (DIP) Manager Risk Evaluation Document (DM RED) 2026-27

Document owner	Document number	Date	Document status
DIP Manager	**V1.0**	**10 February 2026**	**Final**

ELEXON

2 M10 Date Confirmed

Contents

DIP Risk evaluation for 2026/2027

To ensure that parties interact with the DIP in line with agreed standards, a dedicated DIP Assurance Strategy has been established. The strategy includes a requirement for the Data Integration Platform (DIP) Manager (DM) to produce the Risk Evaluation Document (DM RED) annually. The DM RED is developed to assess potential Risk Events that could occur during the Performance Assurance Operating Period (PAOP), that aligns with the financial year, that may directly affect a DIP Users ability to fulfil the obligations set out in the DIP Rules.

11 DIP Risks have been identified and are laid out in appendix of this document; these are derived from the obligations set out in the DIP Rules. A DIP Risk is defined as:

A potential failure or issue within a DIP User's processes, systems, or interfaces that may lead to inaccurate, incomplete, delayed, or misrouted data exchange between market participants.

DIP Risk events 2026 – 2027

Risk events describe potential scenarios that may happen through a DIP Year that would affect a DIP Users ability to adhere to the obligations set out in the DIP Rules. Below details six Risk Events that the DIP Manager believes will be the most prevalent during the 2026-27 PAOP.

Risk events can affect multiple DIP Risks; tables are provided for each Risk event that detail how the event may affect the individual Risks. The tables include a severity rating that estimates how much the Risk may be affected by the Risk event. The Risk events described in this document will allow the DIP Manager to determine what mitigations may be required in the for the following PAOP which will be detailed in 2026 -27 DIP Manager Risk Operating Plan (DM ROP).

Capacity constraints and functional gaps in DIP User systems

1.1. The DIP has been operational since Milestone Ten (M10)[1] on 22 September 2025. Since M10, a subset of the industry has been onboarded to the production environment, resulting in message volumes exceeding 1.5 million per day.

1.2. As more DIP Users move to production and Meter Point Administration Number (MPAN) migrations increase, the DIP and DIP User systems face greater pressure to manage message delivery and ingestion.

1.3. Since Milestone Eleven (M11)[2], DIP User systems have experienced issues handling message ingestion during critical periods. This has been observed during 18:00 -19:00 on days where there are large number of MPAN migration messages are being sent and DIP Users systems experience a large quantity of rejections. These rejections and latency issues are likely due to DIP Users not scaling their systems appropriately.

1.4. Consequences of DIP Users not scaling appropriately can manifest in recipient systems rejecting messages, not providing the initial synchronous response in time, or their systems being unavailable. This increases latency across the DIP as these messages are then retried, taking up threads in egress.

1.5. As the Market-wide Half-Hourly Settlement (MHHS) programme approaches further milestones such as Milestone Fourteen (M14)[3] and Milestone Fifteen (M15)[4], there will be a need for new and existing DIP Users to ensure that their systems are scaled to handle the increase in message volumes.

1.6. Further situations have arisen where parties cannot requeue or replay messages via the Application Programming Interface (API). This has led to DIP Users using the inbuilt Portal feature, which is currently limited to only 100 messages. Therefore, some messages will not be able to be replayed/requeued which will affect a DIP Users ability to act on certain business processes.

1.7. As more parties are onboarded to the DIP, many of which are placing reliance on previous testing carried out, these problems will further exacerbate.

[1] M10 - Central systems ready to migrate Meter Point Administration Numbers (MPANs)
[2] M11 - Commencement of the 18-month migration period for Unmetered Supplies (UMS) and Advanced Metered Meter Point Administration Numbers (MPANs)
[3] M14 - All suppliers must be able to access MPANs under the new Target Operating Model (TOM)
[4] M15 - Full transition complete

Risk ID	Title	Severity	Comments
7	DIP Users using API/Webhooks	Medium	DIP Users cannot use the replay/requeue API which is a functional requirement of the DIP.
8	DIP User System Performance	Medium	DIP Users cannot manage ingesting messages during periods of intense traffic. This is causing latency in DIP to suffer.

Table 1 Risks affected by the "Capacity constraints and functional gaps in DIP User systems" Risk event

Erroneous duplicate messages

2.1. The DIP supports the MHHS Target Operating Model (TOM) and is crucial in both message and operational choreography. From M11, Suppliers and Agents have started sending and receiving interfaces through the DIP.

2.2. The DIP Manager has observed that there are instances where messages are erroneously being duplicated due to a mismatch in data from Suppliers and Agents against what is present in Licensed Distribution System Operators (LDSOs) systems. An example of this has been seen when Data Services send duplicate IF-021[5] messages in error.

2.3. Consequently, the number of messages flowing through the DIP increases, with peak days seeing over an additional 1 million messages.

2.4. For DIP Users, who are receiving these messages, they will need to ingest the messages and conduct suitable validation. This will reduce system performance across the DIP ecosystem, which may lead to downstream operational issues.

Risk ID	Title	Severity	Comments
8	DIP User System Performance	Low	Duplicated messages have not been causing issues with DIP or recipient system yet. As the volumes of messages increase there will be greater computational stress on the DIP user system which may lead to performance issues.

Table 2 Risks affected by the "Transition to operational" Risk event

Lack of validation and status messages

3.1. As part of the MHHS programme design, the DIP requires recipients to send back status messages to the original sender of an interface if there is an issue with the message structure and/or content.

3.2. This can be sent through the DIP as a synchronous response, also referred to as Level 3 (L3) response, or in the asynchronous response, also referred to as Level 4 (L4) response. The DIP Rules and DIP Manager place no preference on whether the participant validates at L3 or L4; however, all validation must occur.

3.3. In the production environment, DIP Manager is seeing unsuitable use of status messages. This can be erroneous status messages or missing status messages. This creates knock on effect to the business processes that these interfaces support.

[5] Settlement Period Consumption Data

3.4. DIP Manager has also identified that there is no defined process for dealing with status messages after they have been received by the DIP User.

3.5. There are a limited number of DIP Users onboarded to the DIP Production environment, as the number of DIP Users increases, there will be more interfaces sent via the DIP, subsequently more of these status messages will need to be sent correctly.

Risk ID	Title	Severity	Comments
1	Incomplete or Failed DIP Onboarding	Medium	Testing does not include “unhappy path” testing therefore there is insufficient evidence on whether DIP Users can create and send status messages for real business cases
6	DIP Message delivery/latency	High	Some DIP Users cannot properly create/send/process status messages

Table 3 Risks affected by the “Ambiguity surrounding use status messages” Risk event

Co-ordination of industry changes

4.1. The MHHS programme brought in the largest change to the electricity industry since privatisation. MHHS has introduced new interfaces and a new TOM, both of which have been formally adopted and subject to enhanced scrutiny since M10.

4.2. The DIP has been designed to support the introduction of new interfaces. The introduction of new interfaces will be dictated by changes initiated by BSCCo and RECCo (or any other Code Bodies that would like to develop processes that require interfaces). The DIP Manger will then support through the DIP Manager change process.

4.3. The message content of an interface is owned by the respective Code Bodies. The DIP Manager then translates the business need of the message into DIP Swagger.

4.4. As this process has yet to be completed outside of oversight of the MHHS programme it creates uncertainty for DIP Users. DIP Users, currently do not have a timeframe form when a change is raised by either BSC or REC to the introduction of a new interface.

4.5. As more interfaces are added, there will be further testing requirements for parties who are coming in as new entrants via the enduring qualification process and for existing parties who wish to use the interfaces. This may require DIP User resource at a time when capacity is already constrained.

Risk ID	Title	Severity	Comments
1	Incomplete or Failed DIP Onboarding	Medium	As new interfaces are introduced there will be a need to increase testing requirements on DIP Users/DIP Applicants
5	Data Management	Medium	The addition of new interfaces creates further requirements for DIP Users to have clear data management principles. New interfaces may have more personal data.
6	DIP Message delivery/latency	Low	DIP Users will need to ensure the validation they are completing aligns with the standards expressed in the DIP Rules. This may include adding new response codes in line with business needs.

7	DIP Users using API/Webhooks	Low	DIP Users need to ensure that when sending a message, they are sending it to the correct API. DIP Users need to ensure their webhooks for configured to receive said message.
8	DIP User System Performance	Low	As new interfaces are introduced this will increase the traffic across a DIP Users system. DIP Users need to ensure that their systems are configured to scale accordingly.

Table 4 Risks affected by the “Co-ordination of industry changes” Risk event

DIP Portal limitations

5.1. DIP Manager has taken ownership of the production environment from the MHHS programme since M10. As the volume of messages has increased, there have been several limitations identified. These include:

5.1.1. Limited requeue/replay functionality. The portal has a limit of 100 messages to requeue from and cannot be filtered to a second-level granularity. Parties are relying on this functionality when their systems cannot ingest all messages. However, at times of heavy traffic, such as the IF-36 period, there are over 100 messages flowing per second.

5.1.2. Limited search functionality in the sent messages tab. The sent messages tab has 350 messages limitations, cannot filter on successful messages or failed messages and cannot search more than one MPAN at a time.

5.1.3. Performance dashboards providing only surface-level reports. The performance dashboard only shows aggregated level data and cannot be ‘drilled down’. This limits the identification of messages that fail at either the DIP level or the recipient level.

5.1.4. Status messages from DIP need to be clearer. There are times when the DIP will not send a status message, causing senders to unnecessarily resend messages.

5.2. This is leading to DIP Users having to place additional resources to identify issues with messages.

Risk ID	Title	Severity	Comments
6	DIP Message latency/delivery	Low	Due to the limited search functionality within the DIP Portal, DIP Users are unable to quickly triage message failures. This issue is further compounded by the limited level of detail available in the performance dashboard.

Table 5 Risks affected by the “DIP Portal limitations” Risk event

Next steps

6.1. DIP Manager will present the DM RED to DIP Change Advisory Board (DCAB). Following this the DIP Manager will publish the DM RED on the DIP Website[6].

6.2. The DIP Manager will then subsequently publish the Annual Assurance Report as well as a draft version of the DIP Manager Risk Operating Plan (DM ROP).

[6] Data Integration Platform assurance - Elexon

6.3. The draft DM ROP will then be consulted on by industry, during that period DIP Manager will take feedback from industry on both the DM RED and the DM ROP and make any necessary adjustments.

Appendix

Appendix 1 - DIP Risk Register

Risk ID	Category and reference	Title	Description	Issue	Mitigations	Obligation
1	**Connection and Operation** DSD002 Section 2	Incomplete or Failed DIP Onboarding	Risk that a DIP Applicant does not complete onboarded activities successfully and/or in a timely manner. Code Bodies do not inform the DIP Manager of Qualification completion.	Prevents access to DIP, halting participation. Affects code qualification. Delay migration of Metering System IDs (MSIDs)	Structured onboarding processes with guidance provided to DIP Users. Functional and non-functional checks completed in coordination with Code Bodies ahead of promotion to production. DIP drop-in session fortnightly offered to DIP Applicants during migration	a) DIP Applicants agree to comply with DIP Rules. b) DIP User using a Certificate Admin from a third party (DCP or other) are responsible for ensuring that the third part Certificate Admin complies with all relevant aspects of Digital Certificate management as set out in the DIP Rules. c) DIP Users must sign Access Agreement ahead of onboarding. d) DIP User must complete relevant testing ahead of onboarding and provide evidence. e) DIP Users must demonstrate ISMS compliance as part of onboarding
2	**Security** DSD002 Annex 2 Section 6 DSD002 Annex 3 DIP-PKI Policy	Certificate Management	The Risk that a Digital Certificate is created, maintained or revoked incorrectly. Risk that a Digital Certificate is compromised due to poor DIP User processes.	Potential data breach, denial of service or malformed/fraudulent messages sent.	Extensive guidance to support certificate creation. DIP Manager has the capability to revoke of certificates. DIP User controls on both GlobalSign Atlas portal and DIP Portal. Separate Certificates across different environments, introduction of API Stop/Start functionality	a) a DIP User will have appropriate certificate setup depending on their organisation setup. b) a DIP User will revoke certificates when required to c) DIP User will be responsible for the generation of TLS keys and CSRs used by their Message service interface d) DIP Users need to submit a CSR which is complicit with the DIP Rules e) DIP Users are responsible for managing and securing their certificates f) DIP Users need to verify domains
3	**Security** DSD002 Annex 2 Section 4	Private Key Management	Risk of Private Key compromised by DIP User or DCP.	Identity spoofing, fraudulent/malformed messages sent, undelivered messages	DIP Manager has the capability to revoke of certificates, introduction of API Stop/Start functionality	a) DIP Users shall follow the DIP-PKI policy b) DIP Users bear responsibility for the use and security of the Private Key associated with a Digital Certificate. c) a DIP User using a DCP is ultimately responsible for ensuring the DCP complies with the DIP-PKI Policy.

	DSD002 Annex 2 Section 10 DSD002 Annex 3 Section 5.9 DSD002 Annex 3 Section 6.9		Risk that digital signatures are not created correctly.			d) DIP Users must ensure that the security of the private key is protected appropriately with a valid form of protection. e) DIP Users, who are natural persons, must be authenticated to their cryptographic module before the activation of the Private Key.
4	**Security** DSD002 Section 3.2.1, 3.2.2 DSD002 Section 6.2 DSD002 Annex 1 Section 1.1.1 (e)(f) DSD006 Section 2.2	Cybersecurity	The Risk that a DIP Users system introduces malware or causes a cyber security incident. Risk of cyberattack on DIP infrastructure.	Platform disruption, data exposure, fraudulent/malformed messages sent, undelivered messages	DIP Users have ISO27001 certification or equivalent, Checks conducted by DIP Manager at onboarding, introduction of API Stop/Start functionality Self-attestation, annual Code of Connection SAD, audit requirements.	a) DIP Users shall undertake Penetration Testing and vulnerability management testing routinely in accordance with Good Industry Practice and ISO 27001 requirements') DIP Users shall maintain a Cyber Incident response plan which may be part of a crisis management plan, and which may also be comprised in wider organisational plan. b) DIP Users need to submit their Cyber Incident Plan to the DIP Manager as part of the DIP Managers assurance activity. c) DIP User shall periodically test their Cyber Incident response plans (where relevant in line with the ISO 27001 requirements). The results of such tests shall be retained for a minimum of 5 years and shall be presented to the DIP Manager when required. d) DIP User needs to demonstrate compliance with ISMS requirements at DIP Onboarding and as part of assurance and audit regimes. e) DIP Users when changing ISMS policies from what is presented in documentation need to provide at least one months' notice and a proposal for how they shall meet the compliance
5	**Security** DSD002 Section 3.2.1, 3.2.2 DSD002 Annex 1 Section 1.1.1 (e)(f) DSD006 Section 2.3	Data Management	Risk that a DIP User does not handle data correctly. Risk that a DIP User's system causes a data breach	ICO fines, reputational damage	Ofgem's Data Best Practice Guidance, introduction of API Stop/Start functionality	a) DIP Users shall adhere to the Authority's 'Data Best Practice Guidance'. b) DIP Users need to provide information relating to how DIP Users are complying with DIP data rules c) DIP Users does not have data protection policies and controls under ISMS practices d) DIP Users when changing data protection policies from what is presented in documentation need to

	DSD006 Section 3.4					provide at least one months' notice and a proposal for how they shall meet the compliance
6	**Technical** DSD002 Annex 2 Section 7 DSD002 Annex 2 Section 9 DSD002 Annex 2 Section 11.4.2	DIP Message delivery/latency	Risk of DIP message loss or corruption in transit. Risk of message not being sent	Settlement and operational errors due to messages not processed in prescribed times or at all.	TLS encryption, digital signatures, message validation and replay APIs	a) DIP Users need to encode JSON messages using UTF-8 format. b) DIP User will need to send messages to channel specific endpoints c) DIP Users' systems, depending on role need to provide an asynchronous response in suitable time. d) DIP Users' systems, depending on role need to provide an initial synchronous response in suitable time. e) On receipt of message a DIP User should endeavour to validate the message contents as much as feasibly possible and relay all validation errors back to the Sender f) DIP Users will need to be aware they are receiving obfuscated data on specific channels g) DIP Users need to apply message signatures for most messages in order to send message into DIP. h) DIP Users on receipt of a message, need to verify message signatures i) DIP Users are expected to adopt a retry with exponential back off (up to a configurable maximum wait time) if there is a failure in connecting to the DIP.
7	**Technical** DSD002 Annex 2 Sections 9.1 & 9.6	DIP Users using API/Webhooks	Risk of APIs and webhooks not working correctly. Risk that DIP Users do not use APIs or webhooks correctly	Messaging downtime or duplication	API key rotation, retry logic, exponential back-off, monitoring	a) DIP Users need to send messages to valid Api. b) DIP User when sending a message will be responsible for message construction, message addressing, message signing, API Call, API response, back off and retry and managing multiple connections. c) DIP Users when receiving a message will need to validate this in two forms synchronous and asynchronous. d) DIP Users will utilise the replay and re-queue API appropriately e) DIP User will configure Webhooks suitably
8	**Technical** DSD002 Annex 2	DIP User System Performance	Risk of DIP infrastructure overload or underperformance	Delayed or dropped messages,	Performance benchmarking, DIP scalability planning,	a) DIP Users' systems shall have the capacity to process messages according to the following volumes:

Section 11.3 11.4, 9.8.1, 8.13	during peak volumes as a result of DIP User systems. The Risk that DIP User systems cannot handle DIP messages during peak volumes.	potential processing failures if messages fail to deliver after retries	DIP Performance reports.	i) Average daily volume of 66,000 messages/day ii) Peak daily volume of 300,000 messages/day iii) Average hourly volume of 2,750 messages/hour iv) Peak hourly volume of 35,000 messages/hour v) Annual volume of 24,000,000 messages/year. b) DIP Users need to alert DIP Manager when their system will be unavailable. c) DIP Users shall not plan routine outages during the period where the Registration service is processing secured active messages d) All DIP User systems (excluding for the handling of Excludes IF-021) shall provide an initial synchronous response to a message within the following timeframes: i) up to average hourly volume, mean response time of 2s or less ii) up to average hourly volume, 90th percentile response time of 4s or less iii) from average hourly to peak hourly volume, mean response time of 5s or less iv) from average hourly to peak hourly volume, 90th percentile response time of 8s or less. e) All DIP Users' systems (except those stated in sections 11.4.3 and 11.4.4 below) shall provide an asynchronous response (Level 4 validation) to a message within the following timeframes: i) up to average hourly volume, mean response time of 6s or less; ii) up to average hourly volume, 90th percentile response time of 12s or less; iii) from average hourly to peak hourly volume, mean response time of 10s or less; iv) from average hourly to peak hourly volume, 90th percentile response time of 16s or less. Risk of DIP infrastructure overload or underperformance during peak volumes.

						The Risk that DIP User systems cannot handle DIP messages during peak volumes.
9	**Financial** DSD005 Section 4.5 DSD005 Section 4.9 DSD004 Section 3.3	Late/Failed Payments by DIP Payees	Risk that DIP Payees do not pay	Cash flow issues, emergency funding requirements	Late payment default shares, bad debt recovery clauses, credit monitoring	a) DIP Payees need to pay for DIP Costs. b) Any costs associated with the release of DIP Manager Data may be recoverable from the DIP User requesting that data. c) Any costs associated with Change Requests will be recovered by DIP Payees
10	**Connection and Operation** DSD002 Section 3 DSD002 Section 4	Incorrect DIP Off-Boarding	Risk that a DIP User is off boarded incorrectly. Risk that a DIP User is suspended incorrectly.	Loss of service for DIP User	Structured offboarding processes, coordination with Code Bodies, communication with DIP User	a) DIP User does not inform DIP Manager of date in the case of voluntary off boarding. b) DIP User in all cases of offboarding will need to pay of any remaining balance.
11	**Connection and Operation** DSD002 Section 4 DSD002 Section 5	Supplier of Last Resort, Special Administration Regime, and Trade Sales	Risk that the DIP manager does not route DIP messages from a previous Supplier to the SoLR	Messages missed by SoLR, industry disorganisation	Structured SoLR processes, coordination with Suppliers and Authority	a) In the case of a Trade Sale DIP User needs to alert DIP Manager as soon as possible to coordinate with Authority and Code Bodies