ELEXON

DIP Manager Escalation Guidance Note

Date
May 2026

Document owner
DIP Manager

Paper number
V1.1

Synopsis

This guidance note informs DIP Users about the framework that the DIP Manager has developed to escalate DIP User for non-compliance.

1. Introduction

1.1. The DIP Manager, as per DSD003[1], is required to provide assurance against DIP Users. The DIP Manager takes a risk-based approach regarding assuring DIP Users in the Production Environment.

1.2. The purpose of this guidance note is to inform DIP Users about how the DIP Manager may escalate instances of non-compliance with the DIP Rules[2].

1.3. The actions the DIP Manager will undertake for DIP User Assurance are based of the provisions within the DIP Rules.

2. Escalation determination

2.1. The DIP Manager has laid out an investigation phase[3] whereby non-compliance of the DIP Rules by a DIP Users is identified through various means. The investigation process was developed to support DIP Users and return them to full compliance. However, if the desired outcome is not reached, the DIP Manager has the ability to escalate a DIP User through different routes to promote compliance with the DIP Rules.

2.2. During the investigation phase, the DIP Manager will regularly analyse any findings and determine the severity of the non-compliance in relation to, but not limited to;

- the frequency of the issue (is it a one-off event or part of an ongoing problem;
- the scope of the issue (e.g. security, data, performance, operations and/or onboarding);

[1] DSD003 - Assurance and Reporting - Elexon Digital BSC
[2] Rules and governance – DIP
[3] How we investigate and handle breaches - DIP

- the impacted DIP Users (one or more DIP Users);
- the cooperation of the DIP User(s) (responsiveness in timely a manor);
- the long term affect on the market or other DIP Users;
- the scale of the issue (is it localised to a limited number of DIP Users or does immediate action is needed to protect the overall DIP service); and/or
- other Code Body obligations impact (is a DIP User unable to comply with obligations due to this issue).

2.3. The DIP Manager takes into consideration all findings and quantifies them using the table below to give the issue a non-compliance rating. Impact considers the non-compliance severity (points noted in section 2.2) and the number of messages affected. Duration considers the length of time that the issue has been ongoing with low.

Impact	Duration		
	Low (one week or less)	Medium (one to six weeks)	High (over six weeks)
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium/High	High	Critical

Table 1: DIP Manager non-compliance rating

2.4. It should be noted that a “high” non-compliance rating can be reached before one week if the severity of the issue compromises security, wider industry operations, integrity of the DIP service. This is as at the discretion of the DIP Manager.

2.5. If a situation arises, where a single DIP User has become non-compliant with multiple ‘low’ impact issues, the DIP Manager will reassess the overall impact to see if the cumulative effect has increased the total impact.

2.6. All non-compliances, and subsequently the DIP Users responsible, that reach a “high” non-compliance rating will be considered for escalation.

3. Escalation process

3.1. Once a non-compliance has been rated as “high” or above, the DIP Manager will consider if escalation is required to support the DIP User getting back to compliance with the DIP Rules. All escalations will be considered on a case by case bases and a bespoke route of escalation will be developed to ensure the most effective support. Table 2 details the different routes of escalation the DIP Manager may take.

Escalation route	Description
DIP Manager escalation	The DIP Manager will escalate internally to a senior member of the DIP Manager team.
Code Body escalation	The DIP Manager will inform the relevant Code Body or Code Bodies where a DIP User is not complying with the DIP Rules and the issue affects wider code obligations.

Authority escalation	The DIP Manager shall engage with the Authority where the non-compliance is material or substantial, where standard performance assurance methods are not enough or where the issue creates wider regulatory concern.

Table 2: DIP Manager Escalation routes

3.2. A DIP User may be escalated for multiple non-compliances; the DIP Manager may consolidate DIP Assurance activity to relieve burden on activity required by all parties.

3.3. Below are the details of what a DIP User can expect if they have been escalated via the three routes.

3.3.1. DIP Manager escalation: DIP Users will receive an email addressed to a senior member of the DIP User company explaining why the non-compliance is being escalated. The DIP User will be invited to attend a meeting with a senior member of the team DIP Manager to discuss the matter. The DIP Manager will present evidence of non-compliance and the reference in the DIP Rules. The DIP User is then expected to present evidence that they will address the issue. This will be agreed upon with the DIP Manager.

3.3.2. Code Body escalation: If the findings in section 2.2 determines that a DIP User (whilst in breach of the DIP Rules) is possibly in breach of another Code Bodies obligations that they are qualified under, then the DIP User will be escalated to the relevant Code Body DIP User. As a DIP User, the DIP Manager will email the DIP User informing them that the non-compliance has been escalated to a Code Body. The respective Code Body will determine how the non-compliance will be managed under their performance assurance processes. If it is material, they may decide to separately engage with the DIP User. The DIP Manager will support Code Body activities, as an advisory function. The DIP Manager will continue engaging with the DIP User to mitigate the DIP risk.

3.3.3. Authority escalation: the DIP Manager may choose to escalate to the Authority. As a DIP User, you will receive an email from the DIP Manager informing you of this decision. The DIP Manager will work with the Authority to best mitigate the risk or return the DIP User to compliance with the DIP Rules.

4. Avoiding escalation as a DIP User?

4.1. Where a DIP User or the DIP Manager identifies a non-compliance, a DIP User should engage regularly with the DIP Manager about the non-compliance and steps to resolution. This can be done by raising a case in Elexon Support. The DIP Manager may reach out to the DIP Users using the following email DIPManager@elexon.co.uk.

4.2. The DIP Manager expects a DIP User to take positive action, whether that is clarifying the requirement with the DIP Manager or committing to a date with a fix to bring them into compliance.

4.2.1. When situations arise where a multi-step deployment is required to bring a DIP User into compliance, then a DIP User, as best practice, should communicate with the DIP Manager with updates.

4.3. As a DIP User, if you are in the process of escalation, the expectation is to adhere to the guidance of whoever is managing the escalation.

5. Closure of an escalation

5.1. The closure of an escalation non-compliance is based on the judgment of the DIP Manager, the Cody Body, and the Authority, depending on the escalation route. The DIP Manager will utilise the evidence presented by non-compliant DIP Users as the basis for judgment. The DIP Manager will assess whether the residual risk

after corrective actions have been applied is suitable. The DIP Manager will then sign off on the closure of the DIP risk. Code Bodies will follow their own procedures to close out their risks.

5.2. The DIP Manager will maintain a diplomatic stance; a precedent will always exist to support DIP Users rather than punish.