ELEXON

MARKET-WIDE HALF HOURLY SETTLEMENT

SERVICE USERS
OPERATIONS MANUAL
V1.2

Document Control

Properties

Owner	Organisation	Email Address
Gary Leach	Elexon	Gary.leach@elexon.co.uk
Last Update	Next Update	Document Classification
8th April 2025	Following SIT Testing	Public

Changes

Version	Date	Author(s)	Comments
DRAFT	14/10/24	Ian Giles & Mark Scott	Initial Draft
Draft v0.1	13/11/24	Ian Giles & Mark Scott	Updates to Change Management Incident Management Test Cases Links Workshop Feedback
Draft v0.2	28/11/24	Ian Giles & Mark Scott	Updated following comments and feedback from Draft v0.1
1.0	8/1/25	Ian Giles & Mark Scott	Updated following comments and feedback from Draft v0.2
1.1	14/3/25	Ian Giles & Mark Scott	Updated following comments and feedback from SIT Testing and MHHS feedback spreadsheet
1.2	8/4/25	Mark Scott	Following further feedback from the Comments Log

Approvers

Organisation	Name	Role
TORWG Acceptance	N/A	N/A
MCAG Endorsement	N/A	N/A

Documents & References

Ref	Item	Location/Name
Policies	Elexon ITIL Polices	TBC
SDD	Service Definition Document – Service Users	https://www.mhhsprogramme.co.uk/uploads/72f30e91-35c2-4df4-b32a-39468f9732d1/Elexon_Service_Definition_Document_v2.4.pdf

LLSD	Low Level Service Design – Service Users	https://www.mhhsprogramme.co.uk/uploads/ad014cea-cf17-4fad-936d-4729042cbb09/Elexon_Low_Level_Service_Design_-_Service_Users_-_v1.1.pdf
Service Management Strategy	MHHS Service Management Strategy MHHS-DEL2124	https://www.mhhsprogramme.co.uk/uploads/e993792e-7590-4947-b759-ce37d67649b1/MHHS-DEL2124_-_MHHS_Service_Management_Strategy_v1.0.pdf

Contents

1 Summary

1.1 Purpose

The MHHS Service User Operations Manual serves as a guide for managing and maintaining systems supporting MHHS. Its purpose is to ensure that IT operations have all the required information to run smoothly, consistently, and efficiently by providing clear, documented procedures and guidelines.

The focus of the document is on how the services are delivered, including the interactions between the different parties supporting MHHS.

It is intended to compliment the previously published SDD and LLSD.

This document has been developed to be consistent with the MHHS Service Management Strategy (MHHS-DEL2124 version 1.0), which sets out the high-level model that industry participants will operate to support the systems, process and services described within the MHHS Target Operating Model and MHHS Design artefacts.

https://www.mhhsprogramme.co.uk/uploads/e993792e-7590-4947-b759-ce37d67649b1/MHHS-DEL2124_-_MHHS_Service_Management_Strategy_v1.0.pdf

1.2 Scope

The scope of this document is limited to the management and coordination of Major Incidents related to systems or processes supporting MHHS that are managed by Elexon.

It does not extend to Major Incidents originating from systems or processes outside of Elexon's management. This distinction is intentionally out of scope and should be covered by the relevant parties responsible for those external systems or processes.

Additionally, this document will not include local work instructions or process flows.

2 Key Definitions

2.1 Special Operations

2.1.1 Industry-Wide Major Incident Management:

This encompasses incidents such as the outage of a key central system (e.g., CSS or DIP) or significant data breaches. These incidents require coordinated response and management due to their impact across multiple services or stakeholders.

The following descriptions have been aligned with the MHHS Service Strategy Document

2.1.1.1 Examples of Significant Data Breach

Breach Type	Description
DIP Credential Leak	Leakage of API credentials for the Data Integration Platform (DIP), enabling unauthorized access to settlement data.
PII Breach	Exposure of Personal Identifiable Information (PII) of consumers, such as names, addresses, or energy usage patterns.
Tampering with Settlement Data	Unauthorized modifications to settlement data, leading to incorrect billing, forecasting, or market imbalances.
Ransomware Attack	A cyberattack encrypts critical MHHS systems like CSS or DIP, demanding ransom for data decryption.
Insider Threat	Malicious activity by an authorized insider accessing or leaking sensitive data, such as market participant details.
Data Exfiltration from Market Systems	Unauthorized data extraction from MHHS systems, such as forecasts, consumption patterns, or settlement results.
Distributed Denial of Service (DDoS)	A coordinated DDoS attack disrupts key services like CSS or DIP, causing outages or delayed settlement processes.
Compromise of Forecasting Algorithms	Hacking or tampering with algorithms used for demand and consumption forecasting in settlement systems.
Phishing Attack on Market Participants	Targeted phishing campaigns trick stakeholders into sharing sensitive credentials or data.

2.1.2 BSC-Related Query Handling

Industry stakeholders with queries related to the Balancing and Settlement Code (BSC), including topics like BSC qualification, should direct these to the Elexon Service Desk. The Elexon Service Management team will be responsible for addressing BSC-related inquiries raised by any Market Participant within the MHHS TOM framework. Queries unrelated to the BSC should continue to be directed to the appropriate Code Body.

2.1.3 Definition of an Industry-Wide Major Incident

An industry-wide Major Incident refers to an event within a Central Service that causes substantial disruption to the normal operations of both the affected Central Service and any interconnected Central Services or Market Participants.

Such an incident necessitates an immediate, high-priority response involving collaboration from at least one or more Central Services and/or third parties linked to these services. Resolution will require participation from entities beyond the MHHS Service Management scope under 'Normal Operations.'

The definition of a Major Incident also includes those that significantly impact the MHHS TOM (Target Operating Model) or Settlement processes. Incidents outside the scope of the MHHS TOM or Settlement processes are not covered by this document and should be managed by the relevant parties responsible for those processes.

Further details on Major Incidents are here. Further details on Major Incident Scenarios are here.

2.2 Normal Operations

The electricity central service delivery functions comprise the Elexon Central Services, Data Integration Platform (DIP), Central Switching Service (CSS), Data Transfer Network, and the central service operations supporting smart metering.

In the event of an industry-wide major incident, specific Central Service Providers and relevant Market Participants will work together to resolve the issue, led by the Service Management function of the appropriate Central Service Provider. Further details on Major Incidents are here. Further details on Major Incident Scenarios are here.

The nature of the incident and the services affected will determine which providers and participants are involved, as well as which provider's Service Management function will take the lead. For instance, if the CSS were impacted, the Switching Operator would be expected to lead the resolution. The applicable Service Level Agreements (SLAs) guiding the resolution will be those relevant to the lead provider's Service Management function.

It is important to note that only a Central Service Provider can lead the resolution of an industry-wide major incident. However, these incidents may significantly impact broader stakeholders, such as Suppliers and Licensed Distribution System Operators (LDSOs). Therefore, collaborative efforts to resolve the issue may include not only Central Service Providers but also other Market Participants.

Any event falling outside the scope of 'Special Operations,' as defined above, and outside MHHS's 'Normal Operations' Service Management will be resolved independently by the affected parties, without MHHS Service Management's involvement or notification. This approach minimizes unnecessary engagement by MHHS Service Management and enables other parties to act quickly in their resolution efforts.

2.3 Working Hours

2.3.1 Core

Core working hours are defined as 08.30 to 17.30, Monday to Friday (excluding Bank Holidays), during which Elexon staff are expected to be available to handle routine and high-priority activities. These hours ensure that key tasks, such as data validation, monitoring, and issue resolution, are managed in real time to minimise disruptions.

2.3.2 Non-Core

Non-core working hours fall outside of the standard core hours, encompassing evenings, weekends, and public holidays. During these periods, Elexon will operate in a monitoring and support capacity.

Essential tasks, such as system monitoring, alert responses, and critical incident management, will be maintained to prevent any service degradation.

3 Getting Support

3.1 Contact Us & Service Hours

Support Website	Telephone
https://support.elexon.co.uk/csm	03700 106950

Hours of Cover
• Definition of Work Hours is here • Elexon Service Desk will be available 24/7/365. • There is further detail in this document defining Central Service Providers Hours of Cover

3.2 Elexon Service Levels

A response is defined as the initial contact (via the Support Portal, where possible) with a customer to acknowledge the issue, undertake initial troubleshooting, ensure all details are documented and advise the customer of the next steps.

To request an account to access the Portal, please see section Service Portal

3.3 Service Levels for Normal Operations

Elexon Service Levels will apply to Normal Operations (BSC Central Services) as specified in the MHHS Strategy Document; products defined as below

3.4 New Services

- Data Integration Platform
- Industry Standing Data
- Load Shape Service
- Market Wide Data Service
- Volume Allocation Service
- Settlement Operations

3.5 Existing Services

- Central Registration Agent
- Funds Administration Agent
- Central Data Collection Agent
- Energy Contract Volume Aggregation Agent

- Settlement Administration Agent

3.6 Service Levels for Special Operations

During a Major Incident involving 'Special Operations,' Central Service Provider SLAs will take precedence. While Elexon will aim to meet its Normal Operations SLAs where possible, its response will ultimately align with and be guided by the SLAs of the Central Service Provider to ensure a coordinated and consistent approach to incident resolution.

This ensures that all actions are synchronised with the primary service provider managing the issue.

3.7 Incident Classification & Prioritisation

		Impact		
		High *System Wide*	**Medium** *Multiple Users*	**Low** *Single User*
Urgency	**High** *Primary functions not working*	P1 6 Hours	P2 1 Day	P3 5 Days
	Medium *Work functions are impaired but workaround in place*	P2 1 Day	P3 5 Days	P4 20 Days
	Low *Inconvenient*	P3 5 Days	P4 20 Days	P4 20 Days

The impact and urgency will also consider number of consumers and customers impacted, along with any financial impact.

The impact and urgency are assessed by the Service Desk, they are not options that can be selected when logging a case in the portal.

3.8 Elexon Incident Priority Definitions

Priority	Service Level
P1	Complete loss of network infrastructure or systems, or unauthorised data breach due to a security incident or suspected security incident. Unauthorised penetration of customer system(s).
P2	Moderate operational impact on customer system(s) or a security incident/ suspected security incident. Specified and identified threat to the customer system(s).
P3	Minor operational impact on customer system(s) or a security incident/ suspected security incident. Specified and identified threat to the customer system (s).
P4	Service Request

3.9 Elexon Incident Service Levels

Priority	Service Level
P1	For Priority Level 1 Incidents, a work around or enduring fix tested and implemented with 6 hours
P2	For Priority Level 2 Incidents, a work around or enduring fix tested and implemented with 1 Day
P3	For Priority Level 3 Incidents, a work around or enduring fix tested and implemented with 5 Business Days
P4	For Priority Level 4 Incidents (Service Requests), a work around or enduring fix tested and implemented with 20 Business Days

A response is defined as the initial contact (via a telephone call, where possible) with a customer to acknowledge the issue, undertake initial troubleshooting, ensure all details are documented and advise the customer of the next steps.

If another Central Service Provider experiences a Major Incident that does not require any support from Elexon to resolve, we would expect to receive the standard Major Incident updates for awareness.

4 Triage Process

This section, originally defined in the Service Definition Document, has been included here for completeness.

4.1 Triage Process – Process Steps

Number	Action	Description
1.	Case Raised in Service Portal	Service Users will raise a case on the Elexon Support Portal
2.	**1st Line:** Case Management Triage	Each case raised via the Elexon Support Portal is subject to 1st line triage (within 15 mins of raising case). 1st line case management involves verifying if the query is valid for Elexon or requires re-routing. If re-routing is needed, guide the raiser to the correct service desk. If the case has been determined as to be dealt with by Elexon, the 1st Line triage will reassign to the correct function (Incident, Change, Request)
3.	Change	Case is assigned to Change Management and triage process will end here
4.	Incident	Case is assigned to Incident Management and triage process will move to Step 6
5.	Request	Case is assigned to Request Fulfilment and triage process will end here
6.	**SME Triage:** Understand the Incident & its Impacts	If the case is assigned to Incident Management it will then move on to the next level of triage, SME Triage. This Triage will understand the Incident and its impacts

7.	Incident Classification	• Impact Assessment: Evaluate how the incident affects business operations.
		• Urgency Assessment: Determine how quickly the incident needs to be resolved.
		• Priority Matrix:
		  ○ High Impact & High Urgency: Immediate attention, escalate to Level 2 or 3 support.
		  ○ High Impact & Low Urgency: Scheduled resolution, but with attention.
		  ○ Low Impact & High Urgency: Quick fix, but less impactful.
		  ○ Low Impact & Low Urgency: Defer until higher priority issues are resolved.

8.	Service Users	During Technical Triage it is determined if the Incident can be assigned to Internal Elexon Technical Resolvers or engage Service User technical support teams (LDSO, RECCo, DCC etc)
9.	Contact Service User Triage	If in step 8 requires Service User support interaction, the triage team will contact and apply dual triage of the Incident
10.	Engage Technical Resolvers & Product Owner	This involves the appropriate technical experts (resolvers) and the product owner in the incident management process to ensure that the issue is properly addressed.

		Technical resolvers work on diagnosing and fixing the problem, while the product owner provides input on business priorities and impacts,
11.	**Analyse:** Capture & Analyse data/information	This step refers to the gathering of relevant details about an incident and then examining that data to understand the nature, impact, and potential root cause of the issue.
12.	**Contain/Mitigate:** Stop or lower the impact, prevent spread of the issue	This step means implementing immediate actions to limit the damage caused by an incident, reduce its effect on services, and prevent it from affecting additional systems or users while a permanent solution is being developed.
13.	**Remediate/Eradicate:** Fully remove/stop Incident, confirm successful remediation	This step means completely resolving the incident by eliminating its root cause and ensuring that the issue is fully addressed, followed by verifying that the solution is effective, and the incident will not recur.
14.	**Recover:** Recover data & systems, resume business as usual	This step means restoring any lost or affected data and systems to their normal functioning state and ensuring that regular business operations are fully resumed after an incident.
15.	**Review:** Fully remove/stop Incident, confirm successful remediation	This step means evaluating the incident resolution to ensure the problem has been eliminated and verifying that the remediation was successful, preventing recurrence.

5 Incident & Major Incident Management

5.1 Incident Management Definition

Incident Management refers to any unplanned disruption or degradation of service that affects one or more aspects of the settlement processes but does not meet the severity or impact thresholds defined for a "major incident."

This includes Settlement-related incidents and also covers DIP incidents, such as Retail issues, even if they do not directly impact the Settlement Process.

For clarification, the Incident and Major Incident processes apply to Elexon Managed Services only.

5.1.1 Settlement Process Definition

Settlement Process	Description	Impact of Major Incident
Data Aggregation and Collection	Gathering and processing half-hourly consumption data from market participants (suppliers, generators, etc.).	Missing, incorrect, or incomplete data leading to incorrect settlement calculations.
Data Validation	Checking the collected data for accuracy, consistency, and errors.	Widespread validation failures or discrepancies that impact settlement accuracy.
Settlement Calculation	Calculating charges and credits based on validated data, including consumption, generation, and balancing.	Errors in the calculation process leading to incorrect charges or credits for market participants.
Reconciliation and Billing	Ensuring correct financial amounts are billed or credited based on settlement calculations.	Billing errors, incorrect financial data, or delays in processing settlements.
Dispute Resolution and Adjustments	Resolving disputes and adjusting settlement calculations after initial settlement.	Challenges in resolving disputes or implementing adjustments, causing long-term discrepancies.
Timeliness and Compliance	Ensuring settlement processes are completed on time and comply with regulatory requirements.	Delays in settlement processing or missed regulatory deadlines leading to non-compliance or financial penalties.

5.2 Key Aspects of an Incident

Type	Description
Limited Impact	The incident has a limited impact on the settlement process, meaning it does not significantly disrupt core functions or most market participants

Scale	Affects a small number of users, systems, or transactions within the MHHS Target Operating Model
Routine Resolution Path	It is addressed through established incident management procedures, often involving standard troubleshooting, diagnosis, and resolution steps.
No Immediate Regulatory Impact	Unlike major incidents, normal incidents do not immediately threaten compliance with regulatory deadlines or requirements, although they may affect performance if not promptly resolved
Lower Urgency	Normal incidents are usually prioritized lower than major incidents, as their resolution timeframe may not require immediate intervention

5.3 Examples of Incidents

- Minor data discrepancies in non-critical settlement processes.
- Temporary issues affecting a limited number of participants.
- Minor delays in routine reporting that do not impact overall deadlines.

5.4 Mandatory Fields – Logging an Incident

The following are the mandatory fields required when logging an incident.

- Category
    - Based on a drop-down list that is under constant review
- Subject
- Description

5.5 Raising an Incident with Elexon

Number	Action	Description
1.	Case Raised in Service Portal	Service Users will raise a case on the Elexon Support Portal
2.	Review & 1st Line Case Management Triage	Each case raised via the Elexon Support Portal is subject to 1st line triage (within 15 mins of raising case). 1st line case management involves verifying if the query is valid for Elexon or requires re-routing. If re-routing is needed, guide the raiser to the correct service desk. If the case has been determined as to be dealt with by Elexon, the 1st Line triage will reassign to the correct function (Incident, Change, Request)
3.	Major Incident Candidate	A major incident candidate in the incident management flow is an incident that has the potential to cause significant disruption to critical services, requiring immediate evaluation and possible escalation to major incident status for prioritised response and resolution.
4.	Major Incident	If step 3 has been determined as a Major Incident, then the Incident Management flow ends, and the Major Incident

		Management process is started. Please click this link for the Major Incident Process Steps
5.	Technical Triage & Attempt to Resolve	This Triage will understand the Incident and its impacts and will attempt to apply a technical fix to resolve if possible
6.	Triage Resolution	If the Technical Triage resolves the Incident, then move to step 9
7.	Engage Technical Resolver & Product Owners	If the Technical Triage is unable to resolve the Incident, then it will Engage Technical Resolvers and Product Owners. Technical Resolvers and Product Owners can ne internal to Elexon or External Service User as part of the MHHS Target Operating Model
8.	Send Update Comms	Update Comms are issued to the Service Users who has raised the case, this communication will be via the Service Portal, which will also send an email update on the status of the Incident
9.	Resolved	If the Incident at this point is resolved, then move to step 14.
10.	Review Incident & Attempt Resolution	If the Incident is not resolved, then the Technical Resolver will review the Incident to attempt a resolution
11.	Change Required	As part of the Incident resolution, a Change may be required, if not move to step 13.
12.	Change Management	If a Change is required, the flow now moves into the Change Management process flow
13.	Resolved	Once a resolution has been applied (either via a technical solution applied or Change Management process) this step confirms the resolution
14.	Send Resolution Comms	Once resolution has been confirmed, resolution communications is sent via the Service Portal
15.	Resolve Incident	The case that has been raised will then be moved to the resolve status in the ITSM toolset
16.	Incident Report	Post Incident and after the resolution, an Incident report will be created to review the fix and determine if a problem record needs to be created
17.	Problem Record	If as part of the Incident Report a Problem Management ticket needs to be created, if not, the flow ends
18.	Problem Management	If a Problem Management ticket needs to be created, this moves to the Problem Management flow and this process ends

5.6 Key Aspects of a Major Incident

Type	Description
High Impact	The incident affects critical settlement processes or a substantial number of market participants, potentially causing significant delays or inaccuracies in settlement activities.
Wide Scope	Affects core functions, systems, or large-scale data within the MHHS Target Operating Model, with potential impact to downstream processes.
Immediate Regulatory and Compliance Risk	The incident may put Elexon or other market participants at risk of missing regulatory deadlines or breaching compliance requirements.

Heightened Urgency and Priority	Major incidents are prioritised at the highest level and typically require immediate action, dedicated resources, and rapid escalation.
Formal Communication Protocol	Elexon's Service Management team initiates formal incident communication channels to keep all stakeholders, including market participants and regulatory bodies, informed of the incident status, resolution efforts, and impact assessments.
Specialised Major Incident Management Process	Elexon follows a structured major incident management process (please refer to Service Definition Document for process flow and actions)
Financial Impact	A major financial impact involves significant monetary losses to market participants, such as suppliers or consumers. It can also include large-scale billing or settlement errors, resulting in incorrect charges or missed payments, and disruptions to settlement processes that lead to financial instability or disputes across the market.
Health & Safety	A major health and safety incident involves MHHS failures causing harm or risks to life, such as power disconnections for medical equipment or widespread outages affecting public safety.
Vulnerability	Situations where a lack of access to critical systems or data creates barriers for vulnerable consumers to manage their energy usage effectively, exacerbating financial or physical challenges.

5.7 Distribution List

Please refer to Appendix – Distribution List

5.8 Major Incident Triage

How a Major Incident is raised and assessed and who can raise a Major Incident and how these are initially triaged.

Action	Description
Logging	The incident is logged in Elexon's Support Portal detailing initial information such as: • Date and time of detection • Systems affected • Observed symptoms • Initial severity assessment
Verification of Major Incident Status	Elexon's service management team assesses the incident to verify whether it meets the criteria for a major incident (high impact, regulatory risk, etc.).
Classification	Based on initial findings, the incident is classified as a major incident, distinguishing it from lower-priority issues.
Impact Assessment	Elexon evaluates the scale of the incident to understand its impact on: • Core settlement processes • Number and types of affected market participants • Financial Impact • Downstream or interdependent systems

Action	Description
Severity and Urgency Assessment	This phase includes determining the urgency level, based on factors like: Extent of disruption to settlement activities Time sensitivity (e.g., risk of regulatory deadline breach)
Regulatory and Compliance Risks	Assess if there's a risk of non-compliance with regulatory obligations.
Stakeholder Notification and Escalation	**Internal Escalation:** Elexon activates its internal major incident management team, involving specialists, technical leads, and senior management. **Stakeholder Communication:** Key stakeholders, including affected market participants and regulatory bodies, are notified according to a predefined communication protocol. This includes: • Initial incident briefing • Estimated time to resolution, if known • Advice on interim measures for affected participants
Assignment of Major Incident Manager and Triage Lead	**Major Incident Manager:** Elexon assigns a dedicated incident manager who will oversee the incident resolution and coordinate resources. **Triage Lead:** A triage lead is appointed to handle ongoing assessment and adjust priorities if the incident evolves.
Prioritisation of Actions and Resource Allocation	**Resource Allocation:** Assess the impact of the incident on both Settlement and Retail areas, engaging industry participants to understand the disruption caused by the DIP outage. **Prioritisation of Actions:** Implement temporary fixes or workarounds to minimise the impact of the DIP outage, with industry participants following guidance to limit disruptions. Focus on full restoration of services, root cause analysis, and long-term fixes. Industry participants will be informed and may assist with testing or providing required data. **Disaster Recovery Plan (if needed):** If core systems (including DIP) are severely impacted, initiate disaster recovery to restore service continuity, with industry participants involved for business continuity, such as performing manual transactions or alternative processes. Service continuity.
Ongoing Monitoring and Real-Time Updates	**Real-Time Monitoring:** The incident manager and triage team monitor real-time data to track the incident's progression and effectiveness of the resolution steps. **Continuous Communication:** Regular updates are provided to stakeholders, detailing any changes in the resolution timeline, adjustments in priority actions, and progress toward incident resolution.
Resolution and Post-Incident Review	**Resolution Verification:** Once resolved, the incident is validated to ensure all affected systems are back to normal operation. **Post-Incident Analysis:** A post-incident review (PIR) is conducted to assess: • Root causes and contributing factors • Effectiveness of the response and triage process

Action	Description
	• Improvements to prevent similar incidents in the future **Documentation and Reporting:** Final documentation is completed, and a report is shared with stakeholders, summarising the incident, resolution, and any recommendations for future prevention.

Please refer to Engagement Communications for further information on Engagement Details

5.9 Validity Checks

Major Incident Validity Checks are a set of predefined assessments carried out to determine whether an incident qualifies as a "major incident" under service management criteria.

These checks involve evaluating the incident's impact, severity, and scope — such as the number of affected stakeholders, disruption to critical services, or potential regulatory implications.
Below is a set of Validity checks Elexon will apply for Major Incident Management:

Type	Category	Description
Impact on Settlement Processes	Critical Process Interruption	The incident disrupts core settlement processes essential to MHHS, such as data processing, calculation, or reporting, which impacts daily or monthly settlement cycles.
	Major Data Integrity Issues	Significant data discrepancies or corruption that compromise the accuracy or reliability of settlement data.
Scope and Scale of Affected Market Participants	High Number of Participants Affected	The incident affects a substantial portion of market participants (e.g., multiple suppliers, generators, or distribution networks), hindering their ability to participate in the settlement process.
	Geographical or Segment Spread:	The incident affects multiple regions or segments of the market, indicating widespread impact across different areas or participant types.
Regulatory and Compliance Risk	Risk to Regulatory Deadlines	The incident poses a clear threat to meeting mandatory regulatory timelines, such as month-end settlement deadlines or compliance reporting dates.
	Non-Compliance Risk	Failure to resolve the incident promptly could lead to a regulatory breach, resulting in penalties, market

Type	Category	Description
		sanctions, or other compliance issues for Elexon or participants.
Severity of Service Disruption	Significant System Downtime	The incident causes prolonged downtime or unavailability of critical systems that support the MHHS TOM.
	Severe Performance Degradation	Even if systems remain operational, performance degradation severely limits functionality, slowing down data processing or transactions and impeding market operations.
Urgency and Restoration Complexity	Extended Resolution Time Expected	If initial assessment indicates that the incident will require extensive time to resolve due to complexity, interdependencies, or resource needs, it may justify elevation to Major Incident status.
	Complex Recovery Requirements	The incident may require disaster recovery procedures, specialized expertise, or significant resource allocation to restore services, suggesting an elevated response level.
Security or Cybersecurity Concerns	Data Security Threat	If the incident involves potential or confirmed data security risks, such as a data breach, unauthorized access, or potential compromise of sensitive data, immediate promotion to Major Incident status may be warranted.
	Cyberattack or Threat Detected	A confirmed or suspected cyberattack on critical infrastructure or systems that support MHHS TOM would likely trigger escalation to Major Incident status.

5.10 Example Thresholds and Triggers

Using the above criteria, Elexon's service management will apply thresholds or triggers for escalation, such as:

- Impact Threshold
  - Affecting more than 10% of market participants or a critical settlement function.
- Duration Threshold
  - Expected resolution time exceeds standard SLAs by 50% or more.
- Compliance Risk Threshold
  - Any incident that risks non-compliance with regulatory obligations.
- Security Threshold
  - Any confirmed or suspected security breach affecting settlement data integrity.

5.11 Summary Process for Validity Checks

5.11.1 Settlement

- Evaluate the incident against each validity criterion.
- Determine if any thresholds are met or exceeded (e.g., impact on market participants, regulatory deadlines).
- If criteria justify it, the incident is promoted to Major Incident status, triggering the major incident management protocol.
- Document the criteria that triggered escalation and inform stakeholders of the incident's new status and response actions.

5.11.2 Data Integration Platform

- Evaluate the incident against the relevant validity criteria for DIP services, considering SLAs and processes outlined in the REC, in addition to Settlement-related impacts.
- Determine if any DIP-specific thresholds are met, such as impacts on Retail processes or REC obligations, alongside standard incident evaluation.
- If DIP-specific criteria justify escalation, promote the incident to Major Incident status, triggering the DIP-specific major incident management protocol.
- Document the DIP-specific criteria that triggered escalation and inform stakeholders of the incident's status, ensuring alignment with DIP-related SLAs and REC processes.

5.12 Major Incident Process Steps

Number	Action	Description
1.	Elexon Service Portal	Service Users will raise a case on the Elexon Support Portal (unless a suspected Cyber Incident, then please call the support number)
2.	Review & 1st Line Case Management Triage	Each case raised via the Elexon Support Portal is subject to 1st line triage (within 15 mins of raising case). 1st line case management involves verifying if the query is valid for Elexon or requires re-routing. If re-routing is needed, guide the raiser to the correct service desk. If the case has been determined as to be dealt with by Elexon, the 1st Line triage will reassign to the correct function (Incident, Change, Request)
3.	Major Incident Candidate	A major incident candidate in the Major Incident Management flow is an incident that has the potential to cause significant disruption to critical services, requiring immediate evaluation and possible escalation to major incident status for prioritised response and resolution.
4.	Incident Management	If step 3 has been determined as an Incident only, then the Major Incident Management flow ends. If this is classified as a Major Incident, then the flow continues to Step 5

5.	Review Promotion Request	Once the Incident has been determined as a Major Incident, the Major Incident Manager will then review the promotion request
6.	Valid Major Incident	After the Major Incident has been reviewed it will be determined if this is a valid Major Incident, if so, move to step 7. If not, this will move to the Incident Management flow and this flow ends
7.	Promote to Major Incident	Once all validity checks have been completed, this will then be promoted to a Major Incident
8.	Initial Comms sent to Major Incident Comms List	Communications to Service Users will be sent using the Major Incident Communications List
9.	Engage Technical Resolver & Product Owners - Establish Bridge Comms	If the Technical Triage is unable to resolve the Incident, then it will Engage Technical Resolvers and Product Owners. Technical Resolvers and Product Owners can ne internal to Elexon or External Service User as part of the MHHS Target Operating Model. Bridge Communications will be established
10.	Send Update Comms	Update Comms are issued to the Service Users who has raised the case, this communication will be via the Service Portal, which will also send an email update on the status of the Incident
11.	Industry Circular Required	This step determines is an Industry Circular is required as part of the communications. If not move to step 14.
12.	Send Industry Circular	An Industry Circular is sent
13.	Update BSC Website (by Incident Manager)	The BSC Website will be updated by the Major Incident Management detailing the Major Incident
14.	Review Incident & Attempt Resolution	The Technical Resolver will review the Incident to attempt a resolution
15.	Change Required	As part of the Major Incident resolution, a Change may be required, if not move to step 17.
16.	Change Management	If a Change is required, the flow now moves into the Change Management process flow
17.	Resolved	Once a resolution has been applied (either via a technical solution applied or Change Management process) this step confirms the resolution
18.	Industry Circular Required	This step determines is an Industry Circular is required as part of the communications. If not move to step 21.
19.	Send Industry Circular	An Industry Circular is sent
20.	Update BSC Website (by Incident Manager)	The BSC Website will be updated by the Major Incident Management detailing the Major Incident resolution
21.	Send Resolution Comms	Once resolution has been confirmed, resolution communications is sent via the Service Portal
22.	Resolve Incident	The case that has been raised will then be moved to the resolve status in the ITSM toolset
23.	Major Incident Report	Post Major Incident and after the resolution, a Major Incident report will be created to review the fix and determine if a problem record needs to be created
24.	Problem Record	If as part of the Major Incident Report a Problem Management ticket needs to be created, if not, the flow ends
25.	Problem Management	If a Problem Management ticket needs to be created, this moves to the Problem Management flow and this process ends

5.13 ServiceNow Status Options

Below are the ServiceNow Status Options with definition and usage.

Type	Definition	Usage
New	The incident has been created but not yet assessed or assigned.	This is the initial status when a major incident is logged.
In Progress	The incident is actively being worked on.	Indicates that a team is investigating or resolving the issue.
On Hold	Work on the incident has been paused temporarily. This would also pause any SLA clock running. **Subcategories**: Awaiting Caller, Awaiting Change, Awaiting Problem, Awaiting Vendor	This may be due to waiting for additional information, vendor support, or other dependencies.
Resolved	The incident has been addressed and a solution has been implemented.	This status indicates that the incident is resolved but may still need to be validated or confirmed by the user.
Closed	The incident has been fully resolved, and all related tasks and follow-ups are complete.	This status is applied once all necessary actions are taken, including communication with the affected users.

5.14 Example Major Incident Workflow

- New → (Assessment) → In Progress
- In Progress → (Dependency Check) → On Hold
- On Hold → (Receive Input) → In Progress
- In Progress → (Resolution Implemented) → Resolved
- Resolved → (Validation) → Closed

5.15 Major Incident Scenarios

Please go to Appendix for full details of Scenarios

5.16 ServiceNow Resolver Groups

Please go to Appendix for full details of Resolver Groups

5.17 ServiceNow Category Drops Downs

Category	Incident Category Description
Settlement Services	Incidents related to core settlement functions.

Category	Incident Category Description
Data Submission	Issues concerning data submitted by participants or collected via systems.
Market Systems	Technical issues related to the systems supporting the MHHS.
Participant Issues	Issues reported by market participants, such as suppliers, generators, or data providers
Data Aggregation and Reporting	Incidents related to aggregation, reporting, or reconciliation of market data.
Regulatory Compliance	Issues related to ensuring compliance with regulatory requirements for market settlements.
Security	Security-related incidents affecting MHHS operations or participant systems.
Communications	Issues regarding communication channels or notifications.
Change Management	Incidents arising from planned or unplanned changes in the system.
Third-Party Services	Incidents related to third-party systems or services supporting the MHHS process.

5.18 Engagement Communications

Description	Action	Communication
Case Raised in Elexon Support Portal	Service Users submit a case via the Elexon Support Portal, describing the issue and its impact	• Automated alert sent to Service Management team, notifying them of the new case. • Acknowledgment email to Service User, confirming receipt of the case.
1st Line Case Management Triage	First-line support assesses and categorises the case within 15 Mins Case is routed to the appropriate function	• If classified as a Major Incident, an immediate escalation is triggered, notifying the Incident Manager, Product Owner, and relevant stakeholders.
Major Incident Management Engagement	Major Incident Manager begins the incident management process.	**Initial Incident Notification** • Recipients: MHHS TOM stakeholders, Product Owners, Elexon senior management, and relevant service teams. • Method: Email and portal notification. • Content: Brief incident summary, initial impact assessment, and confirmation of escalation to Major Incident.
SME Triage - Understanding the Incident and Impact	Subject Matter Experts (SMEs) review the incident, assess impact, and urgency.	**SME Triage Update** • Recipients: Incident Manager, Product Owners, and key technical stakeholders. • Content: Update on preliminary findings, scope of impact, and urgency level.
Incident Classification and Priority Assignment	The incident is classified based on impact and urgency. Classification is determined in the	**Priority Notification** • Recipients: Relevant technical resolver teams, Product Owner, and Incident Manager.

Description	Action	Communication
	following area of this document	• Content: Assigned priority level, impact details, and any immediate actions planned.
Technical Triage - Assignment to Internal or Service User Resolvers	Determination of whether the incident requires internal Elexon teams or Service User support (e.g., LDSO, RECCo, DCC).	**Resolver Assignment Notification** • Recipients: Assigned technical resolver teams, Incident Manager. • Related Industry Participants • Content: Assignment details, description of issue, and any support required from Service Users.
Dual Triage Engagement with Service User Support (if needed)	Contact Service User support teams and begin joint investigation.	**Engagement Notice** • Recipients: Service User support team, internal technical resolvers, Product Owner. • Content: Description of the incident, required input from Service User, and contact points.
Engagement with Technical Resolvers and Product Owner	Technical resolvers and Product Owner engage in the incident resolution process, providing insight on technical and business impacts.	**Technical Collaboration Meeting** • Timing: As needed, often every 30 minutes in a "war room" format. • Participants: Incident Manager, Product Owner, and key technical teams. • Content: Updates on technical findings, proposed solutions, and alignment on business priorities. • Related Industry Participants
Data Capture and Analysis	Technical teams gather and analyse data to identify the root cause.	**Analysis Update** • Recipients: Incident Manager, Product Owner, and senior management. • Content: Preliminary analysis findings, identified impact, and estimated time to resolution.
Containment and Mitigation Efforts	Immediate containment actions are implemented to limit the incident's impact.	**Mitigation Update** • Recipients: All stakeholders, including technical teams, Product Owners, and affected Service Users. • Content: Description of containment actions, current impact status, and expected effectiveness.
Remediation and Incident Resolution	Technical teams resolve the root cause and confirm resolution.	**Resolution Notification** • Recipients: MHHS TOM stakeholders, Product Owners, and senior management. • Method: Email and portal notification. • Content: Confirmation of resolution, summary of actions taken, and statement of restored service.
Recovery	Restore systems and ensure normal operations resume	**Recovery Confirmation** • Recipients: Service Users, Product Owners, technical teams.

Description	Action	Communication
		• Content: Confirmation that services are fully operational, with verification of restored data or systems.
Post-Incident Review (PIR)	Conduct a review of the incident to identify root causes and process improvements.	Further details on Post Incident Review can be found here

5.19 Engagement Communications Summary Overview

Step	Timing	Purpose	Participants/Recipients	Method
Initial Detection & Notification	Immediately upon detection	Notify technical and management teams	Service Management Team, Incident Manager	Automated alert, email
Initial Stakeholder Notification	Within 15 minutes	Inform stakeholders of incident	MHHS stakeholders, Product Owners, senior management	Email, portal notification
SME Triage	As case is escalated	Confirm incident scope and impact	Incident Manager, Product Owners, SMEs	Email, ServiceNow update
Incident Classification	During SME triage	Set priority based on urgency and impact	Technical teams, Product Owners	Email, ServiceNow update
Technical Triage Assignment	Immediately after classification	Assign resolvers and contact Service User if needed	Technical teams, Product Owner, Incident Manager	Email, direct messaging
Dual Triage with Service Users	As determined by triage	Collaborate with Service User technical teams	Internal and external support teams, Product Owners	Conference call
Resolver Engagement Meeting	Ongoing	Coordinate technical troubleshooting and priorities	Incident Manager, Product Owner, Technical Resolvers	Conference bridge
Data Analysis Update	During resolution efforts	Share analysis of findings and root cause	Incident Manager, Product Owners, senior management	Email, ServiceNow update
Containment Update	Ongoing during containment	Inform stakeholders of containment status	Stakeholders, Product Owners, Service Users	Email, portal notification
Resolution Notification	Immediately post-resolution	Confirm incident resolved	All initially notified stakeholders	Email, ServiceNow, portal update
Recovery Confirmation	After full recovery	Verify data/system restoration	Service Users, Product Owners	Email

Post-Incident Review	Details Here	Review and improve incident response	All key stakeholders, technical, and incident management teams	PIR meeting, report email

5.20 Major Incident Communications List

At the time of issuing this version of the Service User Operating Manual, the Major Incident distribution list is not yet available. These details are currently being collected through Elexon-led workshops and information gathered via webforms.

The finalised Major Incident distribution list will be stored and managed within the Elexon Service Management tool and will include the following components:

- **Managing the Distribution List.**
  - The distribution list will be regularly reviewed and updated to ensure accuracy, reflecting any changes in roles or contact details for Service Users and other stakeholders.

- **Communication Methods**
  - Communication methods will be defined for each recipient group, detailing channels such as email, SMS, and the ServiceNow portal for prompt updates throughout the incident lifecycle.

- **eCAB Engagement**
  - The Emergency Change Advisory Board (eCAB) will be involved in critical decision-making processes during major incidents to oversee impact assessments, prioritization, and resolution approvals.

5.20.1 Communications Frequency

Communication Type	Frequency
Initial Notification	Immediately upon incident identification
Regular Updates	Every 30 minutes to 1 hour during investigation
Escalation Notifications	Immediately upon escalation
Resolution Updates	Once resolution is implemented
Post-Incident Review	Within 24 hours after resolution
Follow-Up Review Meetings	Within 1-2 weeks post-incident
Ad-Hoc Communications	As necessary

5.21 Industry Circular

Industry Circulars during IT incidents based on several criteria, primarily to inform stakeholders about disruptions affecting core services like Settlement Administration Agent (SAA) reporting, Balancing Mechanism Reporting Service (BMRS), and data aggregation processes.

Key reasons for issuing these circulars include:

- **Service Disruptions**
    - If there is an incident that impacts the availability or accuracy of settlement or reporting data, such as delays or errors in releasing scheduled reports or system failures, Elexon informs the industry to provide transparency and allow affected parties to take any necessary actions.

- **Resolution Updates**
    - Circulars are also used to communicate resolutions to previous incidents, particularly when data accuracy or critical calculations have been impacted. These updates help industry participants understand when normal service will resume or if interim measures, like using default data, are in place.

- **Urgency and Impact**
    - Circulars are more likely to be issued if the incident significantly affects settlement accuracy or creates potential financial implications for market participants. This aligns with Elexon's approach to maintain industry trust by managing risks proactively and keeping all stakeholders informed.

These criteria ensure that we provide timely and relevant information, helping stakeholders remain informed about critical infrastructure and data flows in the energy market.

5.22 How to get added to Major Incident Comms

Major Incident Comms

To be added to the main Major Incident Comms list, raise a request in the Elexon Support Portal to be added, the process is the same to be removed from the list

There is no limit to the number of people you can have added.

Industry Circulars

To be added to the industry Circulars add your email against the systems you would like notifications for at the BSC status website.

https://status.elexon.co.uk/

5.23 Location of the BSC Website

The location of the BSC Website is as follows: https://status.elexon.co.uk/

Below is a brief overview on the contents of this website

- Information on the latest developments including changes, updates, and timelines.

- Resources related to incident management, problem management, and other operational processes for BSC systems and services.
- Access to key reporting tools and services, such as the Balancing Mechanism Reporting Service (BMRS), Settlement Administration Agent (SAA) reports.
- Details on how to register and comply with BSC rules and regulations.
- Information on ongoing or upcoming consultations and industry changes.

5.24 Post Major Incident Review

Category	Action	Description	Timing – Post Incident
Initial Incident Summary and Context	Assemble Key Stakeholders	Convene a small, focused team of key stakeholders (e.g., incident manager, technical lead, MHHS TOM representatives, and relevant Elexon staff) who were involved or impacted by the incident	2 Hours
	Review Incident Timeline	Document a high-level timeline of the incident, detailing when it was first detected, actions taken, resolution, and impact duration.	
	Outline Scope and Immediate Impact	Clearly summarize the scope of the incident, including which participants or systems were affected, and the overall business impact (e.g., disruption to half-hourly settlement processing, data inaccuracies).	
Root Cause Analysis	Gather Data	Collect relevant logs, reports, and stakeholder accounts to understand what led to the incident	6 Hours (to start within this period. Root Cause Analysis can continue through process will informing next steps)
	Conduct a Rapid Root Cause Analysis	Identify the immediate and underlying causes of the incident.	
	Identify Contributing Factors	Note any secondary factors that contributed to the incident (e.g., system load issues, delayed maintenance)	
Assessment of Incident Response	Evaluate Response Actions	Assess how quickly and effectively the incident response was carried out,	8 Hours

Category	Action	Description	Timing – Post Incident
		including any delays in detection, communication, or resolution.	
	Review Communication Protocols	Evaluate the internal and external communication steps taken during the incident to determine if they were effective in informing stakeholders.	
	Identify Gaps or Inefficiencies	Note any areas where the response could have been faster or more effective.	
Impact Analysis	Assess Market and Participant Impact	Quantify the incident's impact on market processes, participants, and any data integrity issues.	12 Hours
Draft Recommendations and Action Plan	Identify Immediate Corrective Actions	List any corrective measures needed to prevent a recurrence, such as updating systems, adjusting workflows, or enhancing monitoring	18 Hours
	Assign Action Owners and Timelines	Designate responsible teams or individuals for each recommended action and set preliminary deadlines.	
PIR Report Drafting and Stakeholder Review	Create the PIR Document	Summarise findings, root cause analysis, impact assessment, and recommendations in a structured document.	22 Hours
Final PIR Review and Sign-Off	Sign Off	Obtain formal sign-off from relevant leadership to finalise the report.	22–24 hours
	Distribute the Final PIR	Share the final report with relevant internal teams and external stakeholders as needed.	

5.25 Non-Elexon Major Incidents

If an industry-wide major incident occurs, a selection of Central Service Providers and Market Participants will collaborate to resolve the incident. This collaboration will be led by a specific Central Service Provider's SM function. For the definition of Central Service Providers

The nature of the major incident event and the affected services will dictate which Central Service Providers and Market Participants collaborate in the resolution, and which Central Service Provider's SM function leads the resolution. For example, if it was an issue with the Central Switching Service (CSS), it would be expected that the DCC would lead the resolution.

The SLAs that would apply to the resolution of the major incident would be the SLAs that are applicable to the SM function of the Central Service Provider who leads the resolution efforts.

Note that the industry-wide major incident resolution can only ever be led by a Central Service Provider.

However, such issues are likely to have a significant impact on wider parties, such as Suppliers and Licensed Distribution System Operators (LDSOs), and so the collaborative resolution efforts can involve not just Central Service Providers but also wider Market Participants.

6 Problem Management

6.1 Problem Management Definition

Problem Management within Elexon's Service Management framework for supporting MHHS TOM focuses on identifying, analysing, and addressing the root causes of recurring or significant incidents to minimize disruptions and improve service reliability.

This section applies exclusively to BSC-managed processes and systems. For systems or processes outside this scope, Problem Management will be handled by the relevant system/service owner.

6.2 Key Aspects of a Problem Management

Type	Description
Proactive Issue Identification	Continuous monitoring and analysis of incidents to uncover underlying problems early.
Root Cause Analysis (RCA)	Systematic investigation to determine the fundamental causes of issues for effective resolution.
Collaboration with Stakeholders	Engaging market participants, service providers, and internal teams to validate findings and align solutions.
Problem Resolution and Prevention	Implementing permanent fixes or temporary workarounds to minimize impact while addressing root causes.
Knowledge Management	Documenting learnings, resolutions, and preventive measures to enhance future problem-handling efficiency.
Alignment with SLAs and Business Objectives	Ensuring problem management supports service levels.
Post-Implementation Reviews (PIRs)	Evaluating solutions' effectiveness and identifying opportunities for further service improvements.

6.3 Examples of Problems

Problem	Description	Resolution Approach
Data Inconsistencies in Market Submissions	Market participants report discrepancies between submitted and processed data, impacting settlement accuracy.	Conduct RCA to identify systemic issues in data validation processes. Collaborate with participants to refine submission protocols and implement automated data checks.
Recurring Portal Authentication Failures	Users experience frequent login failures, disrupting access to critical MHHS TOM services.	Analyse authentication logs to pinpoint root causes, such as system timeouts or compatibility issues. Deploy fixes and enhance user support documentation.

Delayed Response to Out-of-Hours Incidents	Incident response times are inconsistent during non-business hours, leading to prolonged service outages.	Investigate escalation gaps in out-of-hours support processes. Engage stakeholders to redesign response protocols, ensure alignment with SLAs, and implement training for teams.

6.4 Raising a Problem with Elexon

Number	Action	Description
1	Access the Elexon Support Portal	Log into the Elexon Support Portal using authorized credentials and navigate to the "Raise a Case" section.
2	Submit Problem Details	Provide a detailed description of the issue, its impact on processes, affected systems, and supporting data. Select "Problem" as the case type.
3	Confirmation and Acknowledgment	Receive a unique case reference number and an acknowledgment email confirming the case submission.
4	First-Line Triage	The first-line support team reviews the case within 15 minutes, assesses the issue, and routes it to the appropriate function (e.g., Incident, Change, Problem Management).
5	Initial Evaluation	Evaluate the problem's impact. If significant, escalate to the Major Incident Management process. Otherwise, move to Problem Management.
6	Problem Analysis and Technical Review	Conduct a root cause analysis (RCA) and collaborate with technical resolvers, product owners, or external providers.
7	Communication Updates	Send regular updates via the portal and email to the user who raised the problem, keeping them informed of progress.
8	Resolution or Escalation	Apply a resolution through technical fixes or escalate to Change Management or other specialised workflows if needed.
9	Final Resolution and Confirmation	Document the resolution, send a confirmation to the user, and mark the problem as resolved.
10	Post-Resolution Review	Conduct a review to ensure the root cause is addressed, update documentation, and implement preventive measures to avoid recurrence.

6.5 Problem Management Mandatory Fields in ServiceNow

Field	Description
Problem Number	A unique identifier auto generated by ServiceNow for tracking the problem.
Short Description	A summary of the problem to provide quick insight into the issue.
Description	Detailed information about the problem, including symptoms, impact, and any initial findings.

Priority	The urgency and impact of the problem, often based on predefined criteria.
Category	The high-level grouping or classification of the problem (e.g., software, hardware, network).
Assignment Group	The team or department responsible for managing or resolving the problem.
Assigned To	The specific individual responsible for resolving or investigating the problem.
Impact	The scope of the problem's effect on users, systems, or services (e.g., High, Medium, Low).
Urgency	The speed at which the problem must be addressed, influencing its priority level.
Configuration Item (CI)	The affected system or component from the Configuration Management Database (CMDB).
State	The current lifecycle status of the problem (e.g., New, In Progress, Resolved, Closed).
Root Cause	The identified underlying cause of the problem (mandatory when closing the problem).
Workaround	Details of any temporary solution implemented to mitigate the issue's impact.
Resolution	A clear description of how the problem was resolved or permanently fixed.
Closure Code	A reason for closing the problem, such as "Resolved" or "Known Error."

7 Request Fulfilment

7.1 Method to raise a service request

Step	Type	Description
1	Log In to the Elexon Support Portal: Elexon Support Homepage - Elexon Support	• Go to Elexon Support Portal • Log in with your credentials.
2	Navigate to the Case or Request Creation Section	• On the homepage navigate to Report a Service Issue
3	Fill Out Case Details	• Choose Category: MHHS Service Request • Enter in Subject name of Service Request • Enter in description details of the Service Request • Attach Supporting Documentation
4	Submit Case	• Case is submitted to 1st Line Triage
5	Track and Manage Your Case	• After submission, you can monitor the status of your case from the My Cases.

7.2 Response & Resolution SLA

The below are for Elexon Service Desk only.

Type	Response Times	Resolution Times	Examples
Standard	Within 1 Business Day	Within 5 Business Days	• Routine Access Requests • Standard Account Modifications • Data Extract Requests
Complex	Within 1 Day	Within 5-10 Business Days	• System Configs • Creating New Reports
High Priority	Within 4 Business Hours	Within 1-2 Business Days	• Urgent Access • Configuration Adjustments
Custom	Within 2 Business Days	Custom Timeline	• Integrations with New systems • Enhancements

7.3 Communications Method for Request Fulfilments

Communication Type	Channel	Description
Standard	Service Management Portal	• Real Time • Automated Notifications

Communication Type	Channel	Description
	Email Notifications	• Responses on Submission • Updates • Resolution
	Knowledge Base	• Guides • Instructions • Update Logs
Complex & High Priority	Same as Standard	• See Standard Section
	Phone Support	• For urgent requests that require a quick response
	Incident or Change Notifications	• For complex requests that impact multiple users
Custom	Same as Standard	• See Standard Section
	Kick off meetings	• For request that may require a Project
	Progress Updates	• For custom or project-based request to give an update

8 Change Management

8.1 Change Management Definition

Change Management is the process responsible for managing the lifecycle of all changes to minimize risk and disruption to IT services.

The goal of Change Management is to ensure that standardized methods and procedures are used for handling changes in IT infrastructure, applications, and services to prevent unnecessary interruptions, improve productivity, and maintain service quality.

The Change Process only refers to Elexon Central Systems, with other Central Systems under the TOM operating their own Change Process.

This process does not cover Changes that impact the Code, the following is a link to the BCS Code Change documentation.

https://recportal.co.uk/operational-documents

8.1.1 Key Objectives of Change Management include:

- Ensuring all changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner.
- Minimizing the risk of disruption to IT services while facilitating beneficial changes.
- Providing a consistent and effective approach to evaluating, approving, and scheduling changes.
- Aligning IT services with evolving business needs and compliance requirements.

8.1.2 Types of Changes:

Type	Description
Standard Change	Pre-approved, low-risk, and recurring changes that follow a set process
Emergency Change	Requires immediate implementation due to an urgent need to restore service or prevent potential service impact
Normal Change	Requires risk assessment and approval

8.2 Raising a Normal Change

Changes can be raised by any the following.

Company	Role
Elexon	Service Owners
Elexon	Project Manager
Elexon	Service Providers

8.3 Mandatory fields for the ServiceNow for Change

Type	Categories	Description
Information	Number	The unique identifier for the Change Request. It is auto generated.
	Type	Specifies the type of change, Normal, Standard, or Emergency
	Short Description	A brief, one-line summary of the change.
	Category	High-level classification (e.g., Software, Hardware).
	Description	A detailed description of the change, its purpose, and expected outcome.
Planning & Justification	Reason for Change	Explanation of why the change is necessary
	Risk and Impact Analysis	Assessment of potential risks, which can include fields like risk level and impact level
	Priority	Sets the urgency and business impact of the change, often chosen from a priority matrix.
	Requested By	The person requesting the change, often auto-filled based on the user submitting the request.
Scheduling	Planned Start Date	The anticipated start date and time for the change.
	Planned End Date	The anticipated end date and time for the change.
	Change Window	A specified time frame in which the change will take place, often used for Standard and Normal changes.
Approval	Approval Fields	Approval status and approvers, typically required for Normal and Emergency changes.
Post-Implementation	Change Closure Code	Reason or category for closing the change (e.g., Successful, Unsuccessful).
	Closure Notes	Additional details about the outcome and any issues encountered.

8.4 Risk Matrix

Below is the risk matrix for Change Management.

Impact / Probability	High Risk	Medium Risk	Low Risk
High Probability	**High Risk**	**High Risk**	**Medium Risk**
Description	High probability of service disruption or introducing instability. Involves critical systems, dependencies, or	High probability of disruption, moderate system impact. May involve systems with limited testing or interdependencies,	Low probability of disruption but may still involve interdependencies or slight uncertainties.

	unproven implementations. Requires thorough assessment and contingency plans.	needing careful assessment.	Requires basic assessment.
Medium Probability	**High Risk**	**Medium Risk**	**Low Risk**
Description	Critical systems involved, dependencies present, or lack of proven implementation success. Requires contingency planning.	Routine change with moderate risk due to limited testing or interdependent systems. Assessment required but manageable.	Well-understood processes with minimal likelihood of disruption. Often streamlined approval process.
Low Probability	**Medium Risk**	**Low Risk**	**Low Risk**
Description	Occasional incidents or unpredictable circumstances. Requires careful evaluation and risk mitigation planning.	Routine, low risk change with minimal impact, likely already pre-tested.	Very low probability of issues, with routine or pre-tested processes that pose minimal disruption potential.

8.5 Risk Definition

Risk reflects the likelihood that a change could cause issues, disruptions, or failures, often based on factors like change complexity, time constraints, and previous success with similar changes.

Type	Description
High Risk	• High probability of causing service disruption or introducing instability • Involves critical systems, has dependencies, or lacks a proven history of successful implementations • Requires thorough assessment, and contingency plans.
Medium Risk	• Moderate probability of service disruption or introducing some level of instability. • Generally routine but with some elements that may introduce risk, like limited testing or interdependent systems. • Requires careful assessment
Low Risk	• Low probability of causing issues, often due to well-understood, routine processes or changes that are pre-tested • Minimal impact on services even if something goes wrong • Often qualifies for streamlined approval

8.6 Impact Definition

Impact represents the potential scope and severity of a change on the organization or affected services. ServiceNow typically defines impact in terms of its effect on users, systems, or business functions:

Type	Description
High Impact	• Affects a critical business function or has market wide impact • Likely to cause significant disruption to services or business processes. • Often requires careful planning and high-level approvals due to its potential reach.
Medium Impact	• Affects a limited set of users or a specific application • May cause moderate disruptions, but typically with less extensive business or market wide consequences • Requires moderate oversight
Low Impact	• Affects a minimal number of users or a minor part of the infrastructure. • Causes little to no disruption to business processes. • Often approved through a fast-track or simplified process

8.7 Additional Information

- Should a Change have Low Risk and Low Impact it will not need to obtain CAB approval and will be assessed by the Change Manager.
- Normal Changes not requiring CAB approval should be raised 5 working days ahead of the proposed Change start date.
- Normal Changes requiring CAB approval should be submitted by COB on Tuesday to be reviewed at the CAB the following Tuesday.

8.8 Closing Changes

The Service Provider responsible for the Change implementation should close the change with one of the following Change outcomes.

Type	Description
Successful	The change occurred with no issues
Successful with Issues	The change occurred with a manageable issue, didn't need a high priority incident raised, and produced the intended outcome
Unsuccessful	**Failure to Meet Objectives** The change does not deliver the expected functionality or improvement. **Service Disruption** Causes unexpected outages or degradation in performance of key systems **Incident Generation** Introduces incidents requiring unplanned troubleshooting or rollback. **Ineffective Rollback** Rollback procedures fail, prolonging service disruptions or causing data inconsistencies.
Backed Out	The change was attempted but to avoid failure was rolled back per planned rollback strategy within the planned time frame

Cancelled	The change did not happen; the Change Request was closed without implementation being attempted
Unauthorised	The change was made without authorisation (whether successful or not); also changes with an approved plan that were egregiously executed outside the plan details (e.g. completely outside planned window, changed additional or different CIs, etc.)

Any Change that was closed with any Change outcome other than Successful or Cancelled will follow the Post Implementation Review process.

8.9 CAB

8.9.1 Purpose

The CAB exists to provide advice, risk assessment, and authorization support for changes impacting IT services and infrastructure. It ensures that changes are evaluated for potential risks, impacts, and alignment with organizational goals.

8.9.2 Scope

The CAB assesses and approves Normal changes that have either a risk or impact rating of 1 or 2 and require a thorough review due to their potential impact on IT services, users, or business operations. It excludes Standard Changes, which are pre-approved and follow a separate process, and Normal Changes that are have an impact and risk of 3-Low

8.9.3 Changed Requiring CAB Approval

Type of Change	Description
Major System Updates	Changes to core systems like the Data Integration Platform (DIP), or settlement platforms.
High-Risk Changes	Changes identified as having a high potential for service disruption, such as upgrades to critical infrastructure or changes impacting multiple stakeholders.
Regulatory or Compliance-Driven	Changes required to meet new regulatory requirements (e.g., Ofgem mandates, GDPR updates, or NIS Directive compliance).
Infrastructure Overhauls	Significant updates to underlying infrastructure, such as database migrations, cloud architecture changes, or network reconfigurations.
Service Level Changes	Changes affecting agreed SLAs (Service Level Agreements) or OLAs (Operational Level Agreements).
Introduction of New Services	Implementation of new functionalities, tools, or systems that impact market participants or operational processes.
Cross-Stakeholder Impact	Changes that involve multiple stakeholders, such as suppliers, generators, DNOs, or third-party vendors, requiring coordination and alignment.

Type of Change	Description
Security Enhancements	Implementation of security patches, upgrades, or measures addressing vulnerabilities in critical systems.
Rollback-Dependent Changes	Changes where rollback is complex or carries significant risk, such as schema changes to settlement databases.
Incident Response Changes	Changes to resolve major incidents that require structural updates or enhancements to prevent recurrence.
Operational Policy Updates	Modifications to processes or policies that affect the operational framework of the MHHS TOM.

8.9.4 Objectives

- To ensure that all changes are reviewed for risk, impact, resources, and timing.
- To recommend approval or rejection of changes based on a balanced consideration of risk versus benefit.
- To monitor the progress of changes and post-implementation reviews to improve future change processes.

8.9.5 Responsibilities

- Reviewing and advising on changes, focusing on, significant, or major changes.
- Ensuring that change requests have adequate documentation, risk assessments, testing results, and back-out plans.
- Prioritising changes based on organizational needs and resource availability.
- Providing final authorization for changes when required and escalating to senior management if necessary.
- Participating in post-implementation reviews to identify lessons learned.

8.9.6 Agenda

- Review of the previous meeting's minutes and any action items
- New Change Proposals - Discuss new change requests, including scope, risk assessment, impact analysis, and testing
    - Identify and address any high-priority or critical changes that need immediate attention
- Scheduled Changes - Review and discuss scheduled changes and timelines that are due in the coming week
- Discuss any significant changes that are expected to be raised soon
- Emergency Changes: Analyse any unplanned/emergency changes and their impacts
- Review changes that have been recently implemented and not closed as Successful or Cancelled, and discuss their outcomes, lessons learned, or adjustments required
- Acceptance of new proposed Standard Changes

8.9.7 Membership

At the time of issuing this version of the Service User Operating Manual, the CAB Membership list is not yet available. These details are currently being collected through Elexon-led workshops and information gathered via webforms

- CAB Membership will be a combination of Permanent and Ad-hoc Members depending on the Change.
- If any Permanent Members are unable to attend, they should nominate a deputy to attend on their behalf

Name	Organisation	Role

8.9.8 Meeting Frequency

CAB will convene each Tuesday at 12.00. Emergency CAB will be held as required or may take place during a MIM Bridge call.

8.9.9 Post-Implementation Review (PIR)

The CAB reviews the success and lessons learned from changes for significant and major changes where the Change has not been successful, to inform future improvement.

8.10 Reporting

The following lists the scheduled reports from the Change Management team.

To either be added to, or removed from these reports, please email

SMChangemanagement@elexon.co.uk

The Forward Schedule of Change and Retrospective Change Report will be issued at 6am on a Mondays, the Forward Schedule of Change will include Changes submitted and approved up to that time.

8.10.1 Forward Schedule of Change

Type	Description
Report Title	Forward Schedule of Change
Purpose	To show all changes planned within the next xx day

Frequency	Include frequency and when – weekly, 6am Mondays
Field Descriptions	
Number	The Change reference number
Category	The category of the change
Assigned to	The person that the change is assigned to
Short Description	A field for the short description of the Change
Planned Start Date	Planned start date and time of the Change
Planned End Date	Planned end date and time of the Change

8.10.2 Retrospective Change Report

Type	Description
Report Title	Retrospective Change Report
Purpose	To show all changes that were due to be implemented in the previous week and their status
Frequency	Include frequency and when – weekly, 6am Mondays

8.11 Monthly Reporting

The Change Manager will prepare regular reports on change activity, including metrics on the number of changes, types of changes, success rates, and any issues encountered.

- Number of Authorised vs. Unauthorised changes
- Percentage of reversed or backed-out changes
- Change acceptance rate vs. Rejected changes
- Schedule variance - Schedule variance is the difference between the amount of time a change implementation is expected to take vs. the amount of time it takes.
- Number of incidents/tickets caused by new changes
- Percentage of changes completed on time and budget

8.12 External Parties Notification of Change

Any external parties can send Change Notifications to the Change Team at SMChangemanagement@elexon.co.uk

9 Emergency Change Management

9.1 Emergency Change Management Definition

An Emergency Change is defined as a change that must be implemented urgently, typically to address a high-impact issue, such as an ongoing incident, security breach, or a situation that could cause significant service disruption. Emergency Changes bypass the standard Change Management process due to their critical nature but are still subject to risk assessment and review by an Emergency Change Advisory Board (CAB), to ensure they are safe and effective.

Key characteristics of an ITIL emergency change include:

- Urgency: The change must be implemented immediately to prevent or mitigate significant disruption or damage to services.
- Approval Process: Emergency changes still go through a streamlined version of the change management process, often requiring quick approval from designated senior personnel or an emergency CAB.
- Risk and Impact Consideration: Despite the urgency, the potential risks and impacts of an emergency change are still assessed to ensure minimal disruption to other services.
- Documentation: Emergency Changes are documented thoroughly to provide transparency and enable review after implementation for any necessary corrective actions or process improvements.

The Emergency Change Process only refers to Elexon Central Systems, with other Central Systems under the TOM operating their own Emergency Change Process.

9.2 Mandatory fields for the ServiceNow for Change

Type	Categories	Description
Information	Number	The unique identifier for the Change Request. It is auto generated.
	Type	Specifies the type of change, such as Normal, Standard, or Emergency
	Short Description	A brief, one-line summary of the change.
	Category	High-level classification (e.g., Software, Hardware).
	Description	A detailed description of the change, its purpose, and expected outcome.
Planning & Justification	Reason for Change	Explanation of why the change is necessary
	Risk and Impact Analysis	Assessment of potential risks, which can include fields like risk level and impact level
	Priority	Sets the urgency and business impact of the change, often chosen from a priority matrix.
	Requested By	The person requesting the change, often auto-filled based on the user submitting the request.

Scheduling	Planned Start Date	The anticipated start date and time for the change.
	Planned End Date	The anticipated end date and time for the change.
	Change Window	A specified time frame in which the change will take place, often used for Standard and Normal changes.
Approval	Approval Fields	Approval status and approvers, typically required for Normal and Emergency changes.
Post-Implementation	Change Closure Code	Reason or category for closing the change (e.g., Successful, Unsuccessful).
	Closure Notes	Additional details about the outcome and any issues encountered.

9.2.1 Risk Definition

Risk reflects the likelihood that a change could cause issues, disruptions, or failures, often based on factors like change complexity, time constraints, and previous success with similar changes.

Type	Description
High Risk	High probability of causing service disruption or introducing instability Involves critical systems, has dependencies, or lacks a proven history of successful implementations Requires thorough assessment, and contingency plans.
Medium Risk	Moderate probability of service disruption or introducing some level of instability. Generally routine but with some elements that may introduce risk, like limited testing or interdependent systems. Requires careful assessment
Low Risk	Low probability of causing issues, often due to well-understood, routine processes or changes that are pre-tested Minimal impact on services even if something goes wrong Often qualifies for streamlined approval

9.2.2 Impact Definition

Impact represents the potential scope and severity of a change on the organization or affected services. ServiceNow typically defines impact in terms of its effect on users, systems, or business functions:

Type	Description
High Impact	Affects a critical business function or has market wide impact Likely to cause significant disruption to services or business processes. Often requires careful planning and high-level approvals due to its potential reach.
Medium Impact	Affects a limited set of users or a specific application

	May cause moderate disruptions, but typically with less extensive business or market wide consequences Requires moderate oversight
Low Impact	Affects a minimal number of users or a minor part of the infrastructure. Causes little to no disruption to business processes. Often approved through a fast-track or simplified process

9.3 Closing Emergency Changes

The Service Provider responsible for the Change implementation should close the change with one of the following Change outcomes.

Type	Description
Successful	The change occurred with no issues
Successful with Issues	The change occurred with a manageable issue, didn't need a high priority incident raised, and produced the intended outcome
Unsuccessful	The change was implemented and remains in effect, but significant issues occurred, such as • A P1/P2 or several P3s • One or more problems caused by the change resulting in new problem records being created • Change occurred out of schedule, unless agreed to by the Change Manager (Unauthorised) • An organised rollback was attempted, but failed to reverse the change
Backed Out	The change was attempted but to avoid failure was rolled back per planned rollback strategy within the planned time frame
Cancelled	The change did not happen; the Change Request was closed without implementation being attempted
Unauthorised	The change was made without authorisation (whether successful or not); also changes with an approved plan that were egregiously executed outside the plan details (e.g. completely outside planned window, changed additional or different CIs, etc.)

Any Change that was closed with any Change outcome other than Successful or Cancelled will the follow the Post Implementation Review process.

9.4 Emergency CAB

9.4.1 Purpose

An Emergency Change Advisory Board (ECAB) is convened to assess and authorize high-priority changes to infrastructure or services that require immediate action. The purpose of an emergency CAB is to:

- When an urgent, often unplanned change is necessary to address a critical incident or prevent imminent risks, the emergency CAB expedites the decision-making process. This

board typically includes senior IT leaders and relevant stakeholders, ensuring swift evaluation and approval.

- Emergency CABs carefully assess the potential impacts of the change on other systems, security, and service continuity. Even under time pressure, the emergency CAB evaluates potential risks and ensures that the change is implemented as safely as possible to minimize disruption.
- The goal is to restore normal operations quickly. The emergency CAB prioritizes changes that stabilize essential services, avoiding prolonged downtimes.
- The Emergency CAB also ensures that the change is documented and communicated to relevant teams, so that there's a record for future analysis and a clear line of accountability.

9.4.2 Scope

The ECAB assesses and approves and Change relating to a Major Incident

9.4.3 Membership

The attendees for the ECAB will be dynamic by their very nature and will typically involve members of the Major Incident team working on the incident resolution and if in hours the Change Manager – the Major Incident Manager will have delegated authority for an Emergency Change required out of hours.

9.4.4 Meeting Frequency

As required

10 Service Portal Access Management

10.1 Requesting Service Portal Access

The Elexon Service Portal is configured for Self-Registration, using the following steps

Step	Description
Visit the Elexon Support Portal Website	1. Go to the Elexon Support Portal URL: https://support.elexon.co.uk/csm
Register	2. Look for the **Register an account**
Fill Out the Registration Form – Step 1	3. Complete the Registration form, it will ask you for the below details **4. Full Name** 5. Email Address (use your official email associated with your company or Elexon participant organisation)
Verification Password	6. Click **Get OTP** 7. You will be sent a 6-digit verification password 8. Enter Password to continue with form
Fill Out the Registration Form – Step 2	9. Search for your **organisation name or Party ID** (all participant company names will be pre-loaded) 10. If you do not have a Party ID, click **I do not have a Party ID** 11. Acknowledge By creating an account you confirm that you have read the Privacy Policy and Accept Terms and Conditions
reCAPTCHA verification	12. Please click box **I am not a robot**
Submit	13. Click Submit to confirm 14. After submitting the form, you'll likely receive an email confirmation.

If you encounter any issues during registration, contact Elexon support via the email or phone number provided on the registration page.

10.2 Ticket Updates

Type	Update Type	Description
Automated Email Notifications	Status Updates	Elexon ServiceNow is configured to send automated email notifications to participants whenever there is a status update on their ticket (e.g., "Acknowledged," "In Progress," "Resolved etc)
	Comments and Additional Information	If a support agent adds a comment or requests more information, the system will trigger an email to notify the participant. Participants can also respond via email
Elexon Support Portal Interface	Portal Status View	Although participants may not access ServiceNow directly, they can still log in to the Elexon Support Portal to view the status of their tickets. The portal would reflect status updates from ServiceNow in near real-time.

Type	Update Type	Description
	Ticket History and Comment Threads	Any notes or comments added in ServiceNow can be configured to appear in the portal's ticket history, allowing participants to view detailed updates without needing direct ServiceNow access.

10.3 Ticket Closures

Step	Description
Resolution Completion and Initial Review	• Once the support team resolves an issue in ServiceNow, they will update the ticket with a detailed resolution summary that explains the actions taken, any root cause identified, and any preventive steps implemented. • Elexon Service Management team will review the ticket to confirm that all necessary actions have been completed and that the resolution aligns with Elexon's quality standards and regulatory requirements.
Participant Notification of Resolution	• ServiceNow sends an automated email to the participant informing them that the ticket is marked as "Resolved" and summarising the resolution. This email will invite the participant to review the resolution in the Elexon Support Portal. • The resolution details are also posted in the ticket history within the Support Portal, allowing participants to log in and review the outcome and any actions taken.
Participant Confirmation of Resolution	• Confirm Satisfaction with the resolution, which they can do by responding to the notification email or logging into the portal and marking the ticket as resolved. • Request Further Action if the resolution is unsatisfactory or if they have additional questions. Participants can add comments directly to the ticket through the portal, reopening the case if further work is needed.
Ticket Closure	• Once the participant confirms that the issue is resolved or if no response is received after follow-up reminders, the support team proceeds with final ticket closure. • The ticket status is updated to "Closed" in ServiceNow, and the participant receives a final email notification confirming the ticket's closure. • If no response from the participant is received within 5 days, the ticket will be automatically closed by ServiceNow
Reopening Process for Closed Tickets (if required)	• If the participant later identifies that the issue was not fully resolved, they can request that the ticket be reopened. They may do so through the Elexon Support Portal by commenting on the closed ticket or by contacting support via email. • Alternatively, if a reopened ticket is not feasible or practical, a new ticket can be created referencing the original issue to address any further support needs.

10.4 Parent & Child Accounts

As a user of the ServiceNow CSM portal, you can establish parent and child accounts to manage multiple related accounts under a single parent account. This hierarchy allows you to effectively oversee different divisions or subsidiaries.

Elexon will configure account relationships and set appropriate access permissions, ensuring that users from child accounts can only view their own data while allowing parent accounts to see aggregated information from all child accounts.

10.5 Security Statement / Justification

10.5.1 Secure Data Handling and Protection

- The Elexon CSM Support Portal uses robust encryption standards (e.g., TLS 1.2 or higher) to secure data transmission between users and the platform, preventing unauthorised access during data transit.
- The portal enforces strict access controls to ensure that only authorised users can access sensitive information. Role-based access control (RBAC) is in place, limiting data visibility according to user roles and responsibilities.
- The portal complies with data residency and privacy requirements by storing data in approved locations, aligning with GDPR and other data protection standards.

10.5.2 User Authentication and Access Management

- The portal supports multi-factor authentication to add an additional layer of security, ensuring that only verified users can access sensitive data and system functions.

10.5.3 Incident Management and Accountability

- The CSM Support Portal has monitoring and logging capabilities that capture detailed records of user actions and system events. This supports incident tracking, audit trails, and accountability, ensuring that all activities are traceable.
- The portal provides structured workflows for managing incidents, enabling Elexon and users to follow standardized procedures. This consistency improves the speed and effectiveness of incident response, minimising security risks and downtime.

10.5.4 Compliance with Industry Security Standards

- The portal adheres to the ISO/IEC 27001 Information Security Management standard, demonstrating its commitment to managing sensitive information securely and systematically.
- The CSM Support Portal undergoes routine security audits, vulnerability assessments, and penetration testing to identify and remediate potential vulnerabilities proactively.

11 Knowledge Management

11.1 Where to access Knowledge Management – Support Portal - Knowledge Management Search Bar

- Access to our Knowledge Management is via the Support portal (https://support.elexon.co.uk/csm)
- You will be able to search for Knowledge Articles under the section 'Search for FAQs')
- There is a search bar for you to be able to search for the required Knowledge article

11.2 Requesting Knowledge Article

11.2.1 Elexon Glossary

Description	Step
Service User Access & Knowledge Search	• Service Users log in to the Elexon Service Management Portal. https://support.elexon.co.uk/csm) • Service Users select the "Glossary" option from the toolbar. • To locate information, they can use alphabetical filtering, e.g., select "D" for DIP-related Knowledge Management (KM) items. • Service Users review the glossary entries to find answers to their queries. • If relevant information, such as "Tips and best practices for effectively using DIP," is unavailable, proceed to raise a case.
Raising a Case to Request New Knowledge Content	• Go to the CSM Service Catalog - Elexon Support section. • Select the 'Report a Service Issue' option and fill out the form with the following details: • Requested by: Enter the name of the person raising the request. • Organisation Name / Party ID: Enter the organization's name or Party ID. If unknown, select "I do not have a party ID." • Market Participant ID: Enter the Party ID if available, or select "I do not have a party ID." • Category: Select the appropriate category from the drop-down options • Subject: Enter "Add item to Glossary." • Description: Detail the missing information, e.g., "No documentation for searched topic - Tips and best practices for effectively using DIP." • URL or Related Page Section: Insert a relevant URL or section link if applicable.
Submit the Case	• After completing the form, click Submit to create the case.

11.2.2 Support Portal Knowledge Management

Description	Step
Service User Access & Knowledge Search	• Service Users log in to the Elexon Service Management Portal. https://support.elexon.co.uk/csm) • Service Users navigate to the Knowledge Management Search Bar on the portal homepage. • They enter relevant keywords, such as "DIP best practices," to search for information related to their query. • Service Users review search results to locate information that addresses their query. • If relevant information, such as "Tips and best practices for effectively using DIP," is unavailable, proceed to raise a case.
Raising a Case to Request New Knowledge Content	• Go to the CSM Service Catalog - Elexon Support section. • Select the 'Report a Service Issue' option and fill out the form with the following details: • Requested by: Enter the name of the person raising the request. • Organisation Name / Party ID: Enter the organization's name or Party ID. If unknown, select "I do not have a party ID." • Market Participant ID: Enter the Party ID if available, or select "I do not have a party ID." • Category: Select the appropriate category from the drop-down options • Subject: Enter "Add item to Glossary." • Description: Detail the missing information, e.g., "No documentation for searched topic - Tips and best practices for effectively using DIP." • URL or Related Page Section: Insert a relevant URL or section link if applicable.
Submit the Case	• After completing the form, click Submit to create the case.

12 Operations Manual Governance

The Operations Manual will be integrated into the Elexon Change Management for version control to ensure a structured, transparent, and accountable process for updating and managing the manual.

This approach ensures that each revision is properly documented, approved, and communicated to stakeholders, below are the process steps to achieve this:

Process Step	Description
Version Control	Every revision of the Elexon Operations Manual will be assigned a unique version number. A version history will be maintained, including a log of the specific changes made in each version (e.g., section updates, policy changes). This ensures transparency and traceability of all changes over time.
Approval Workflow	Updates to the Operations Manual will undergo a formal approval process before being finalised. This process will involve relevant stakeholders (e.g., Elexon Service Management, Code Bodies, and other governance bodies) to review the changes. Only after obtaining the necessary approvals will the manual be signed off for distribution and implementation.
Stakeholder Communication	Once signed off, updates to the manual will be communicated to all relevant stakeholders (e.g., market participants, Code Bodies, Service Providers). Communication will include a summary of changes, their impact, and access instructions to the latest version. Clear timelines for the rollout of changes will also be provided to ensure smooth implementation.
Audit Trail	A detailed audit trail will be maintained for all updates made to the manual, documenting who made the change, the reason for the update, and when the update occurred. This will be part of the Change Management system, ensuring that all changes are auditable and comply with governance standards.

The approval process will cover the publication of the Operations Manual up to M10 (publication schedule including in the Appendix – following M10, this section will be updated to cover BAU approval.

13 Monitoring and Event Management

13.1 Post M10 Implementation

Below are the steps to the Monitoring and Event Management in place for SIT Testing and expected to go live at M10

Type	Action	Description
Azure Alert Generation and Monitoring	Alert Configuration	Azure Monitoring is configured to track specific performance metrics, thresholds, and availability conditions relevant to Elexon's environment.
	Alert Trigger	When a monitored resource (such as a virtual machine, database, or network component) breaches predefined thresholds (e.g., high CPU usage, network latency, or service unavailability), Azure automatically generates an alert.
	Alert Notification	The alert is then sent as an email notification from Azure to the designated service management team or monitoring team inbox.
Manual Alert Review by Monitoring Team	Alert Verification	The monitoring team reviews the alert email to verify its accuracy, checking if it is a valid, actionable alert and not a false positive. This may involve checking Azure's monitoring dashboard or logs for more context.
	Alert Classification	Based on the nature and impact of the alert, the monitoring team assigns a priority level (e.g., Critical, High, Medium, Low) to guide response urgency.
Email Notification to Service Management Team	Email	If the alert is confirmed to require action, the monitoring team forwards the alert email to the Service Management Team with relevant details, including: • Alert Description • Impact Assessment • Priority Level
Service Management Team Case Creation in ServiceNow	Ticket Creation in ServiceNow	• Incident Summary and Description • Classification and Priority • Assignment • Link to Azure Alert Details - If applicable

13.1.1 Process Summary Steps

Step	Action	Responsibility
Alert Generation	Azure generates and emails alert.	Azure Monitoring

Step	Action	Responsibility
Manual Alert Review	Verify and classify alert	Monitoring Team
Email Notification	Email Service Management with alert details and priority	Monitoring Team
ServiceNow Case Creation	Create a ServiceNow ticket with alert information and assign	Service Management Team
Incident Resolution	Investigate and resolve, updating ticket progress	Support/Technical Team
Ticket Closure	Finalise ticket, notify monitoring team, and reset alert	Service Management Team
Post-Incident Review	Conduct RCA if needed and document improvements	Support Team & Monitoring

13.2 M10 Readiness

The Azure Monitoring will have full integration into ServiceNow for M10 Readiness.

Alerts generated by Azure will automatically create and update ServiceNow tickets in real time, eliminating manual intervention and enabling immediate response to potential issues.

14 Service Reviews & Reporting

14.1 Service Reviews

Embedded below is the Terms of Reference related to Service Reviews and Reporting

Elexon Service Management - Terms

14.2 Request a Report

Step	Action
Access the Service Management Portal	Log into the Elexon Service Management Portal
Raise a Case for One-Time Report Request	From the Portal Drop Down Menu, select the "Report a Service Issue" option.
Complete the Required Fields in the Case Submission Form	Enter your full name in the "Requested by" field.
Organisation Name / Party ID	Enter your Organization Name or Party ID in the appropriate field.
Market Participant ID	Enter the Market Participant ID or Party ID. If you do not have a Party ID, select "I do not have a Party ID".
Category	From the Category drop-down menu, select the relevant category for your request. Categories are defined in 4.15 Categories
Subject	Enter "Report Request" in the Subject field.
Description	Please can you supply Report XX
Submit the Case	After completing all the fields, click Submit to raise the case.

A list of stanard reports is in Section 18.6

14.3 Reporting

The monthly report for Elexon Service Management will provide a concise summary of key performance data, incident details, service level adherence, and other relevant updates for the MHHS TOM service. Below is a list of report content:

Content	Description
Executive Summary	Overview of key findings, significant incidents, and high-level performance trends for quick reference.
Service Performance Metrics	**Availability:** System uptime and availability statistics. **Reliability:** Summary of any service outages or disruptions
Incident and Problem Management	**Incident Summary:** Total number of incidents, categorized by severity (e.g., critical, high, medium, low).

	Top Incidents: Details on high-impact incidents, including root cause, resolution time, and any potential preventive actions **Problem Trends:** Analysis of recurring issues or patterns that may indicate underlying problems.
Service Requests and Changes	**Service Requests:** Volume and types of service requests, response times, and any bottlenecks. **Change Requests:** Number of change requests, types of changes (normal, standard, emergency), and any impact on service delivery.
SLA Compliance	**SLA Adherence:** Summary of SLA metrics, highlighting any breaches or near misses and their causes. **Penalty Avoidance:** Overview of any SLA breaches with financial or operational implications
Stakeholder Feedback	**Customer Satisfaction Scores:** Feedback from stakeholders, if collected, on the quality and responsiveness of service. **Feedback Summary:** Summary of specific feedback received (e.g., from surveys or stakeholder discussions).
Risk and Issue Register	**Open Risks:** Current risks related to service operations, with mitigation status. **Critical Issues:** Any critical issues or areas of concern that require attention from management or stakeholders.

14.4 Reporting SLA

SLA Component	Objective	Details
Initial Acknowledgement	Confirm receipt of reports/queries	• Automatic acknowledgment within 15 minutes of submission.
First Response	Provide initial feedback on the report	• Service Desk team response within 24 business hours.
Status Updates	Keep Service Users informed on case progress	• Minor Issues: Update every 48 business hours. • Moderate Issues: Update every 24 business hours.
On-Demand Updates	Allow users to request additional information	• Respond to on-demand update requests within 48 business hours
Resolution Target	Complete reports and resolve inquiries	• Minor/Moderate Requests: Resolved within 5 business days. • Complex Requests: Timelines provided on a case-by-case basis.

15 Service Level Management

15.1 Category dropdowns on the portal (when requesting amendment to existing SLA)

Category	Description	Example Use Case
SLA Amendment Request	Used when a Service User requests an update or amendment to an existing SLA.	Request for changes to response times for Service Reporting.
SLA Review Request	Used for requesting a formal review of current SLAs.	Review of SLA for incident response and resolution times
SLA Clarification	Used when clarification on specific SLA terms or conditions is needed.	Clarification of the escalation process under the SLA for major incidents
SLA Compliance Issue	Used when there are concerns that the agreed SLAs are not being met.	Service reporting SLA not being met as per agreed timelines
New SLA Request	Used for requesting the creation of new SLAs for new services or processes.	Request to create a new SLA for the new reporting feature in MHHS
SLA Documentation Update	Used for suggesting or requesting updates to SLA documentation.	Update the SLA documentation to include new response time targets
Performance Metrics Amendment	Used for modifying or proposing new performance metrics in SLAs.	Propose changes to the service uptime metric in the SLA
Impact Assessment Request	Used when changes to SLAs may affect other processes or systems.	Request an impact assessment for proposed SLA amendment

15.2 Service User requests Service Management Reports

Step	Action
1. Access Portal	Log in to the Elexon Support Portal.
2. Select 'Report a Service Issue'	Choose the appropriate service catalogue option.
3. Choose Category	Select the relevant category (e.g., SLA Performance Report Request).
4. Submit Request	Provide details like subject, description, and additional information.
5. Triage and Assignment	Service Management reviews the case and assigns it to the appropriate team.
6. Report Generation	Assigned team creates the requested report.
7. Delivery & Confirmation	Report is delivered, and confirmation is sent.
8. Feedback & Close	Gather feedback and close the request.

16 Supplier Management

16.1 Suppliers

Elexon collaborates with the following key suppliers to deliver solutions that support the deployment of new BSC Central Services:

- CGI
- Avanade
- Cognizant
- BJSS

16.2 Routine Monitoring and SLA Compliance Tracking

16.2.1 Daily and Weekly Monitoring:

The Service Management team monitors vendor performance daily, tracking adherence to SLAs, incident resolution times, and service availability.

16.2.2 SLA Compliance Check

- At the end of each week, review SLA compliance reports generated to document any breaches and escalate unresolved issues as per escalation protocols.
- Elexon will engage vendors immediately to resolve minor SLA breaches, ensuring that corrective actions are implemented without delay.

16.2.3 Monthly Performance Review Meetings

- Before each monthly performance review, prepare a summary of the vendor's performance, including SLA adherence, incident management, and any notable achievements or issues.
- Share this summary with vendors at least one week before the meeting so they can prepare responses or explanations for any areas of concern.
- Discuss the following items in the monthly performance review meeting:

16.2.4 Review of key KPIs and SLA compliance.

- Status of incidents and problem resolutions, including root causes for significant incidents.
- Progress on continuous improvement initiatives or planned service optimizations.
- Any operational or service challenges encountered by either party.
- Feedback from Elexon stakeholders on vendor performance.
- Document meeting minutes, agreed actions, and deadlines for follow-up.

16.2.5 Follow-Up on Action Items:

- Track all action items resulting from the monthly review. Ensure each item is addressed by the agreed deadline and follow up with vendors as needed.
- For any unresolved issues, escalate according to Elexon's escalation process.

16.3 Incident and Problem Management

- Track incidents daily and review all incidents managed by vendors, ensuring they follow the established incident management and escalation protocols.
- For major incidents, conduct an immediate review and request a Root Cause Analysis (RCA) from the vendor, followed by corrective action.
- Review recurring incidents in monthly meetings to determine if they indicate underlying problems that require resolution.
- Encourage vendors to engage in joint problem-solving sessions for issues affecting multiple systems or users, and document solutions in the knowledge base for future reference.

16.4 Change and Release Management

- Monitor all change requests submitted by vendors, ensuring they follow the standard change management process (e.g., approvals, testing requirements).
- Review changes in weekly or bi-weekly change coordination meetings, assessing any risks or dependencies, and avoiding conflicting changes.

16.5 Post-Implementation Review (PIR):

- Conduct PIRs for major changes to evaluate the change's success and any issues encountered.
- Document lessons learned from PIRs to improve the change management process and avoid similar issues in future changes.

16.6 Compliance and Risk Management

- Schedule quarterly compliance checks to ensure vendors adhere to regulatory requirements (e.g., data security, GDPR).
- Confirm that vendors maintain up-to-date documentation on compliance practices and meet all contractual obligations

16.7 Risk Assessments and Mitigation:

- Periodically assess risks related to each vendor's services, including data security, operational dependencies, and business continuity.
- Work with vendors to develop mitigation plans for identified risks and review these plans as part of the quarterly evaluations.

16.8 Reporting and Documentation

- Produce detailed monthly and quarterly performance reports summarizing vendor performance against KPIs, incident handling, SLA compliance, and any significant issues.
- Share these reports with relevant Elexon stakeholders to maintain transparency and accountability.

16.9 Roles and Responsibilities in Vendor Management

- **Vendor Manager:** Oversees daily operations, leads monthly/quarterly reviews, manages SLA compliance, and coordinates escalation and issue resolution with vendors.
- **Service Management Team:** Supports monitoring, escalation, change management, and facilitates incident/problem tracking.
- **Vendors:** Responsible for day-to-day service delivery, meeting SLAs, providing RCA for incidents, participating in reviews, and implementing agreed improvement initiatives.
- **Elexon Stakeholders:** Provide feedback on vendor performance and participate in the annual review process as needed.

17 DIP Security and Certificate Administration (GlobalSign)

The link below is for Code of Connection document for the DIP Service Interface, defining the interface usage requirements and responsibilities for Market Participants to securely exchange information, it also defines the operational context and constraints in which the DIP Interface

Including

- DIP Security Requirements
- Guidance on the use and management of Public Key Certificates and associated keys
- The processes to be followed and information to be provided by Parties when registering with the DIP service and requesting DIP certificates from the DIP Certificate Authority
- The processes and procedures for distributing key cryptographic key material, including CSRs and Certificates
- The processes for generation, distribution, use and management of TLS keys and Certificates
- The processes for generation, distribution, use and management of JSON message signing keys and Certificates
- An overview of the DIP User Portal

https://www.mhhsprogramme.co.uk/uploads/3ca02d51-4cfe-4642-b7a0-d8b347bccc87/MHHS-DEL1197_-_Interface_Code_of_Connection_v1.5_CL.pdf

17.1 Managing DIP Certificates

17.1.1 Overview

This section describes in more detail the process for obtaining DIP PKI Certificates as well as the main roles and functions of the PKI service. It details the processes to be followed and information to be provided by DIP Service User when requesting DIP PKI Certificates from the DIP Certificate Authority (DCA).

The DIP PKI Certificate processes will be managed using the DIP User Portal where Certificates will also be distributed.

Any issues with Certificates should be logged through the Elexon Support Portal

DIP Service Users will be responsible for managing and securing the certificates they use to communicate with the DIP, there are four actions in the management of certificate:

- Issuing of certificates
- Revocation of certificates
- Renewal of a certificate – prior to expiry
- Reissue of a certificate

Certificates will be issued from the DCA. The certificates issued by the DCA are currently valid for 398 days which equates to 1 year and a month overlap.

17.1.2 Certificate Issuance

This following sections describes in more detail the process for obtaining DIP Certificates as well as the main roles and functions of the DIP service.

On successful verification of a PKCS #10 Certificate request the DCA will generate a Public-Key Certificate for the DIP Service User's Public Key and place that Certificate within a publicly accessible repository.

17.1.3 Certificate signing requests

The DIP Service User (Certificate Admin) can submit a request for a new certificate by following the process below: To request a new certificate the DIP Service User (Certificate Admin) will use the DIP User Portal to provide a Certificate Signing Request (CSR), the signing will be fulfilled by GlobalSign.

- DIP Certificate Admin can only request certificates through the DIP portal.

Once signed, the certificate is fulfilled and therefore considered as a certificate towards the market participant's quota.

The certificate request completion only works on the server/service where the CSR was generated, should it be completed elsewhere then it will not complete.

Name	Description
Common Name	This value will contain a prefix for the environment and the domain which they are requesting a certificate for. The prefixes will be as follows: • energydip-nonprod – All Non Production environments • energydip-prod – Production environment For example, the following value could be specified: • *energydip-nonprod.marketparticipant.co.uk* • *energydip-prod.marketparticipant.co.uk*
Organisation name	The name of the organisation as specified during Organisational vetting.
City	The city of the organisation as specified during Organisational vetting.
State	The state of the organisation as specified during Organisational vetting
Country	The country of the organisation as specified during Organisational vetting.

17.1.4 Certificate revocation

A certificate may need to be revoked for several reasons.

An approved Certificate Admin can revoke certificates using the DIP User Portal following the process below:

- From within the portal, the DIP Service User (Certificate Admin) navigates to the certificates page, the DIP Service User will be shown their current certificates
- Under the certificate actions option, they can choose Revoke.
    - To revoke a certificate a reason for revocation must be entered selected from a list of possible reasons:
- On submission of the reason, the DIP portal will request the certificate is revoked by the DCA
- The DIP portal will inform the DIP Service User (See section 5.4.3) that the certificate is successfully revoked

Once revoked the certificate will no longer be valid when calling the DIP as either the mTLS or message signing certificate.

Note:

A revoked certificate cannot be reclaimed. A new certificate will be required to replace the revoked certificate and the DIP User Organisations quota of certificates will be reduced by 1 (per certificate revoked).

During the process of mTLS or message signing the Online Certificate Status Protocol (OCSP) is called. The OCSP is a property of the certificate and is an endpoint that specifies the certificate status (valid/revoked).

Reason	Description
Key compromise	If the DIP Connection Providers key has been lost, permanently deleted or if an unauthorized entity has been able to take possession of the key, the certificate must first be revoked before being recreated from scratch with a new key.
Cessation of operation	If the service user ceases to operate, the certificate must be revoked. This reason can only be used by the DIP Manager.
Affiliation changes	This is when a key employee leaves the DIP Service User Organisation. A key employee is an employee that has access to the certificate and associated keys.

Certificate superseded	If a new certificate has been produced for any reason, the old certificate will be superseded and will require revocation
Withdrawal of privilege	The DIP Service User is no longer allowed to access the DIP; therefore, their certificate should be revoked.
Removal from CRL	If a certificate is accidentally revoked for any reason and should not be on the Certificate Revocation List (CRL), that certificate will need to be removed from the CRL. This will be a very rare occurrence.

17.1.5 Certificate Renewal

Prior to expiry a Certificate Admin should generate a new CSR and get it signed via the DIP User Portal, the process for this is the same as 17.1.2 Certificate Issuance.

As all requests for signing come through the DIP portal, the portal will notify the DIP Service User that a certificate is about to expire and therefore that they should generate a new CSR and get it signed via the DIP portal.

Note:

Renewing a certificate does not invalidate the current certificate. The current certificate will remain active for the remainder of the validity period allowing a grace period for seamless transfer.

Notifications of certificate expiry will be sent to the DIP Service User Administrator at the following intervals.

- 90 days prior to the certificate expiring
- 60 days prior to the certificate expiring
- 30 days prior to the certificate expiring
- 1 day prior to the certificate expiring.

The new certificate will start from the date the Certificate Signing Request has been completed and not the date the current certificate expires.

17.1.6 Certificate rekey

If you'd like a copy of your certificate, for example are you installing on multiple servers or devices? Additionally, If you encounter a private key error and cannot fully install your Client Digital Certificate, you can simply reissue your certificate.

Any other issues with Certificates should be logged with the Elexon Service Desk in the normal manner.

18 Appendix

18.1 Future Publication Dates – Until M10

Reviewed Version – 2 weeks following the end of SIT Testing

Reviewed Versions – published ahead of TORWG each month until M10

Each of the sections will then be stored as Knowledge Articles with an owner with a review cycle of every 3 months.

Review means review and if there are no changes a .x version is issued but with the comment "Document Reviewed – no further changes required"

18.2 Example Incident Scenarios

Incident Scenario	Impact	Downtime	Who Raises the Issue	Response	Touch Points / Collaboration
DIP Service Failure (In Hours - Secure Active Window)	DIP secondary routing tables not updated, misrouting of flows	2 Settlement periods (1 hour)	SDS (receiving HTTP error messages)	Manage recovery sequence to avoid misrouting of flows	SDS, DIP Support, Market Participants
DIP Service Failure (Out of Hours)	Impact on incoming consumption and registration data	90 minutes	DIP Monitoring triggers incident report	Evaluate if on-call support is sufficient	DIP Support Teams, On-Call Personnel
DIP Security Incident (Within Working Hours)	Potential downtime due to unauthorized data breach	Undefined	DIP Monitoring triggers incident report	Engage security teams, follow security policies	Security Teams, Incident Response Teams, Elexon Service Management
Single LDSO Failure (In Hours - Secure Active Window)	Delay in PUB responses, secondary routing issue	2 hours	Supplier (non-receipt of PUB responses)	Manual intervention to manage sequencing and recovery	SDS, LDSO, Market Participants
MPRS Software Failure (In Hours -	Registration services cease to function	24 hours	Supplier (non-receipt of PUB responses)	Synchronize EES and MPRS after issue resolution	Elexon Service Desk, St Clements Teams, LDSOs

Secure Active Window)					
CSS System Failure	Registration and meter data retrieval cease to function	Variable (depends on failure)	DCC (TOC diagnostics)	Manage sequencing and volume of registration messages	DCC
VAS System Failure (Helix)	Suppliers and LDSOs do not receive REP003 reports	48 hours (weekdays)	Supplier (non-receipt of REP003 reports)	Flag to Elexon Service Management, engage Helix SD process	Elexon Service Management, Helix SD, Market Participants
MDS System Failure (Helix)	Suppliers and LDSOs do not receive REP002a reports	48 hours (weekdays)	LDSO (non-receipt of REP002a reports)	Flag to Elexon Service Management, engage Helix SD process	Elexon Service Management, Helix SD, LDSOs
LSS System Failure (Helix)	SDS & ADS unable to estimate consumption, delays in IF021	48 hours (weekdays)	ADS (non-receipt of LSS data)	Flag to Elexon Service Management, engage Helix SD process	SDS, ADS, Helix SD
DCC Service Failure (IF-021 Volume Issue)	Failure to issue IF-021s due to high volumes	Half a day (up to 4.5 hours)	DIP (identify increased volume requirements)	Staged recovery to manage message volume profile	DCC, Elexon Service Management, DIP, Helix
ISD System Failure (Helix)	Migration issues, validation failures across processes	48 hours (weekdays)	Newly Qualified Party (lack of migration data)	Work with Helix to restore service and issue new ISD data	Elexon Service Management, Helix SD, Market Participants
Data Acquisition Hub (DAH) System Failure	Backlog of consumption and registration messages	3 hours (peak 5 AM to 8 AM)	Helix internal or DIP monitoring	Engage recovery process to prevent message loss and manage retry logic	Helix SD, DIP, Elexon Service Management, Market Participants
SDS Service Failure (e.g., Callisto)	Missing data in REP003 reports, volume allocation issues	2 settlement days	Supplier (non-receipt of REP003 reports)	Identify recovery sequence for managing volume and backlog	Elexon Service Management, SDS, DIP, Market Participants
EES Service Failure	Inconsistent data between EES and REGs	2 days	Supplier (REGS failures	Synchronize EES with REG	Elexon Service Management,

			due to data issues)	data after resolution	EES Service Desk RECCo

18.3 Resolver Groups

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
Settlement Services	Incidents related to core settlement functions.	Data Processing Errors	Issues related to the half-hourly data aggregation or validation.	Settlement Operations Team / Settlement Data Management
		Settlement Calculation Errors	Errors during the calculation of settlements for market participants.	
		Settlement Runs Delays	Delays or issues with scheduled settlement runs	
		Discrepancy in Settlement Data	Inconsistencies in settlement reports or calculations	
		Exception Handling	Issues with the handling of exceptions in the settlement process.	
Data Submission	Issues concerning data submitted by participants or collected via systems.	Meter Data Submission	Problems with half-hourly meter data submission by participants.	Data Submission and Validation Team / Data Aggregation and Reporting Team
		Missing Data	Gaps in expected data submissions (e.g., missing intervals)	
		Incorrect Data Format	Submissions in incorrect formats or	

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
			incompatible data types.	
		Validation Errors	Errors arising during data validation processes.	
		Re-submission Requests	Requests to resubmit or amend incorrect data.	
Market Systems	Technical issues related to the systems supporting the MHHS.	System Performance	Slowness, high latency, or degraded performance of core systems	IT Operations and Systems Support / Application Support
		System Outages	Complete or partial system outages affecting market operations	
		Access Issues	Problems with logging into or accessing MHHS-related systems or portals.	
		Data Retrieval Failures	Issues retrieving or extracting settlement or participant data.	
		Batch Processing Failures	Failures in automated batch processing related to settlement.	
		Integration Failures	Breakdowns in system integrations	
Participant Issues	Issues reported by market participants, such as	Connectivity Problems	Issues with network connections, VPNs, or secure data	Participant Support Team/Access Management Team

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
	suppliers, generators, or data providers		transfer mechanisms.	
		Data Submission Errors	Errors related to the submission of half-hourly data or other critical inputs.	
		User Access Management	Issues with user access permissions, logins, or roles in MHHS systems.	
		Compliance Issues	Non-compliance with MHHS data or operational requirements.	
		Participant System Compatibility	Problems with participant systems interacting with MHHS central systems	
Data Aggregation and Reporting	Incidents related to aggregation, reporting, or reconciliation of market data.	Data Aggregation Errors	Problems with aggregation of half-hourly consumption data.	Data Aggregation and Reporting Team/Reporting and Analytics Team
		Reconciliation Discrepancies	Issues related to data reconciliation across different settlement periods.	
		Incorrect Reports	Issues with the accuracy or availability of reports generated by the system.	

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
		Reporting Delays	Delays in the generation or distribution of reports.	
		Data Mismatch	Mismatches between different reporting systems or tools.	
Regulatory Compliance	Issues related to ensuring compliance with regulatory requirements for market settlements.	Audit Failures	Failures in audit processes or issues flagged during regulatory audits.	Regulatory Compliance Team
		Non-Compliance Reports	Issues raised by participants or regulators related to non-compliance.	
		Compliance Breach Notifications	Incidents related to breaches of market-wide regulations.	
		Discrepancies in Regulatory Reporting	Errors or mismatches in data submitted for regulatory reporting.	
Security	Security-related incidents affecting MHHS operations or participant systems.	Data Breach	Potential or confirmed breaches of participant or settlement data.	Security Operations Team/Cyber Security Team
		Unauthorized Access	Incidents involving unauthorized system access attempts or actions.	
		Vulnerability Reports	Reports of vulnerabilities	

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
			identified in the MHHS system.	
		Security Patch Failures	Problems related to the application or failure of security updates.	
		Phishing/Social Engineering Attacks	Security incidents where phishing attempts or other social engineering methods targeted MHHS systems or participants.	
Communications	Issues regarding communication channels or notifications.	Notification Failures	Incidents where system alerts, notifications, or reports were not delivered.	Communications and Notifications Support Team/Service Delivery Team
		Communication Delays	Delays in sending important market communications or updates.	
		Participant Communication Issues	Issues with receiving or sending communications between participants and the central system.	
Change Management	Incidents arising from planned or unplanned	Planned System Maintenance	Issues caused by planned maintenance activities.	

Incident Category	Incident Category Description	Subcategories	Subcategory Description	Resolver Group
	changes in the system.	Unplanned Changes	Problems arising from emergency or unexpected changes in the system.	Change Management Team / Release Management Team
		Change Rollback	Incidents requiring a rollback of changes due to failure or errors.	
		Configuration Issues	Problems due to incorrect configurations or failed change implementations	
Third-Party Services	Incidents related to third-party systems or services supporting the MHHS process.	Third-Party System Failures	Incidents due to failures in external systems or services (e.g., data providers).	Third-Party Vendor Management Team
		Vendor Support Delays	Delays in resolution or response times from external vendors.	
		Integration Issues with Third-Party Tools	Problems related to the integration of third-party tools with MHHS systems.	

18.4 Distribution List

At the time of issuing this version of the Distribution list is not yet available. These details are currently being collected through Elexon-led workshops and information gathered via webforms

18.5 Glossary of Terms

Common terms used in MHHS and IT service management.

BAU	Business As Usual
BSC	Balancing and Settlement Code
BSCCo	BSC Company BSCCo (Balancing and Settlement Code Company) refers to the organization responsible for managing the Balancing and Settlement Code (BSC), which governs electricity balancing and settlement arrangements in Great Britain. The BSCCo operates under the brand name Elexon. Key Functions of BSCCo/Elexon: Balancing and Settlement Code (BSC) Administration: • Administers the BSC, ensuring compliance with its rules and regulations. • Manages the processes required to balance electricity supply and demand and settle imbalances. Electricity Settlement: • Ensures that electricity generators and suppliers are financially balanced based on their actual versus contracted energy usage. • Calculates imbalance charges and distributes payments accordingly. Market Operations Support: • Provides tools, systems, and reports to market participants to aid in compliance with settlement processes. • Facilitates modifications to the BSC to reflect market changes or regulatory updates. Stakeholder Engagement: • Works with energy market participants, including suppliers, generators, and distribution network operators (DNOs). • Facilitates industry collaboration and consultation for changes to the BSC. Support for Industry Programs: • Plays a key role in delivering significant industry programs, such as the Market-Wide Half-Hourly Settlement (MHHS) Programme. • Provides expertise and system support to implement new market reforms. Governance Ownership: BSCCo is a non-profit entity owned by the electricity industry but independent of any specific market participant.

	Oversight: It is governed by the BSC Panel, which represents different market stakeholders and oversees its performance.
Central Service Providers	The providers that manage and operate the electricity Central Services, namely Elexon, the DCC, RECCo and ElectraLink
Central Services	The services that comprise the electricity central service delivery functions, namely the Elexon Central Services, Central Switching Service, Data Transfer Network, EES, Smart DSP and the central service delivery functions underpinning smart metering
CSS	Central Switching Service
DCAB	The DIP Change and Advisory Board (DCAB) are a specialist user group whose purpose is to advise the DIP Manager in relation to the Data Integration Platform (DIP) and, in limited circumstances, make determinations.
DCC	Data Communications Company Key responsibilities for the MHHS Programme include: Secure Data Transmission: Enabling reliable and secure communication of half-hourly consumption data between smart meters, suppliers, and authorized parties. System Integration & Testing: Supporting system compatibility and participating in testing to ensure seamless operation of MHHS processes. Security & Compliance: Maintaining data security and ensuring compliance with industry regulations, including GDPR. Infrastructure Support: Providing a scalable, robust communication infrastructure for handling increased data volumes. Stakeholder Engagement: Collaborating with energy suppliers and stakeholders to facilitate a smooth transition to MHHS. Operational Continuity: Managing smart metering operations to ensure consistent, accurate data flow and addressing system issues. Facilitating Innovation: Supporting market flexibility, time-of-use tariffs, and renewable energy integration through accurate data services. Smart Service and Switching Service provider
DCP	DIP Connection Provider
Dependencies	Refer to other tasks, systems, resources, or actions that need to be completed or aligned before the current task can proceed further.
DIP	Data Integration Platform
DNO	Distribution Network Operator. A company licensed to operate and maintain electricity distribution networks within a specific region. DNOs deliver electricity from the transmission network to end users, manage infrastructure (e.g., substations and power lines), connect customers, respond to outages, and plan for future demand.
DSP	Data Services Provider
DTN	Data Transfer Network
ECS	Elexon Central Services
EES	Electricity Enquiry Service
ELS	Early Life Support
ERDS	Electricity Retail Data Service
IDNO	Independent Distribution Network Operator: A licensed operator of smaller electricity distribution networks, often serving new developments or renewable

	projects. Unlike DNOs, which manage regional networks, IDNOs operate within DNO areas, offering competition and alternative services.
Incident	An event that results in an unanticipated interruption in the delivery of a service or a reduction in the quality of a service
ISD	Industry Standing Data
Issue	An issue refers to any situation or event that requires investigation to determine its cause and resolution.
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KA	A piece of content stored in the Knowledge Base to provide information, guidance, or solutions to users. These articles are designed to improve self-service capabilities, reduce reliance on IT support, and enhance knowledge sharing
Knowledge Articles	A piece of content stored in the Knowledge Base to provide information, guidance, or solutions to users. These articles are designed to improve self-service capabilities, reduce reliance on IT support, and enhance knowledge sharing
LDSO	(Licensed Distribution System Operator): An entity licensed to manage and maintain electricity distribution networks in specific regions. LDSOs distribute electricity from the national grid to end users, oversee infrastructure (e.g., substations and lines), connect new customers, respond to outages, and ensure network reliability.
Legacy	The existing arrangements set out under the BSC and REC.
LSS	Load Shaping Service
Major Incident	An incident which occurs within a Central Service and causes significant disruption to both the BAU operations of the originating Central Service and other adjacent Central Services and / or Market Participants, and which demands an urgent, high-priority response requiring involvement from at least one or more Central Service or any third party associated with those Central Services.
MDS	Market-wide Data Service
MHHS	Market-wide Half-Hourly Settlement
MHHS Arrangements	The new MHHS arrangements as set out in the MHHS Core Design Artefacts.
MHHS SM	The service management that will be delivered by Elexon in relation to the Elexon managed services, both new and old – DIP, LSS, CDCA, SAA etc.
MIMM Bridge Call	A structured call mechanism used to coordinate responses to major incidents—typically critical disruptions to services or operations that require immediate resolution. • Facilitate real-time communication among stakeholders during a major incident. • Ensure swift coordination to minimize downtime and impact. • Provide a single point of communication for all involved parties.
MPAN	Meter Point Administration Number
MPRS	Metering Point Registration System
NFR	Non-Functional Requirement

Primary Function	The core roles or responsibilities of a market participant or system within the settlement process. These functions ensure accurate, timely, and efficient settlement of electricity usage based on actual half-hourly consumption data.
REC	Retail Energy Code
RECCo	(Retail Energy Code Company): A not-for-profit organization managing the Retail Energy Code (REC), which sets rules for Great Britain's retail energy market. RECCo oversees market processes like supplier switching, promotes competition and innovation, and focuses on improving consumer outcomes, supporting efficiency and the transition to net zero.
Registration Service	Central Registration Service (CRS) the Service operated by the DCC which includes the Central Switching Service (CSS) and Switching Service Desk. The service operated by Centra; Service Switching Provider (CSS)
Response	A response is defined as the initial contact (via a telephone call, where possible) with a customer to acknowledge the issue, undertake initial troubleshooting, ensure all details are documented and advise the customer of the next steps.
Service Desk	The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and handles communication with the users.
Service Providers	Types of Service Providers in the MHHS Context: Metering Services: Providers of advanced metering infrastructure (AMI) to enable half-hourly data collection. Data Aggregators: Entities responsible for aggregating and transferring settlement data. IT Solutions Providers: Firms that deliver technical systems to facilitate seamless integration into the MHHS framework. Consultancy Firms: Advisers on the MHHS transition strategy and compliance. By contributing to the MHHS Programme, these service providers play a critical role in transforming the electricity market, enabling better demand-side management, supporting renewable energy integration, and improving market transparency.
Service Request	A formal request from a user asking the service provider to offer something e.g. a request for information, approval or advice.
Services (The)	Refer to the services and systems supported by Elexon • Data Integration Platform • Industry Standing Data • Load Shape Service • Market Wide Data Service • Volume Allocation Service • Settlement Operations • Central Registration Agent • Funds Administration Agent • Central Data Collection Agent • Energy Contract Volume Aggregation Agent • Settlement Administration Agent
SIT	Systems Integration Testing

SLAs	Service Level Agreements
SM	Service Management
SM Portal	A self-serve platform which users can visit to raise requests and retrieve information
SM Service Provider	The Central Service Provider that would provide the Service Management wrap around the Central Systems they are responsible for
SM System	The tool used by the SM Service Provider to support the delivery of the SM. The system will be used to manage incidents and service requests and provide knowledge.
SMRS	Supplier Meter Registration Service
TOM	Target Operating Model
UMS	Unmetered Supplies
UMSO	Unmetered Supplies Operator
VAS	Volume Allocation Service
Vendor	The Elexon suppliers providing the technical capability to delivery MHHS
Work Function	A specific set of activities or tasks performed by a role, system, or organization to support the MHHS process. These functions are part of the operational or technical workflow that enables the collection, validation, processing, and settlement of half-hourly electricity consumption data.

18.6 Standard Reports Available

Incident Management

- Open Incidents by Assignment Group
- Incidents Resolved Per Assignment Group
- Aging Incidents (Grouped by Age Buckets)
- Open Incidents by Priority
- Mean Time to Resolution (MTTR) for Incidents
- Incidents by Category and Subcategory
- First Call Resolution Rate

Change Management

- Open Changes by State
- Change Requests by Type (Normal, Emergency, Standard)
- Change Requests by Assignment Group
- Changes with Unauthorized CI Modifications
- Scheduled Changes

Request Management

- Open Requests by Type
- Requests Fulfilled by Category
- Request Fulfillment Time by Assignment Group
- Backlog of Service Requests

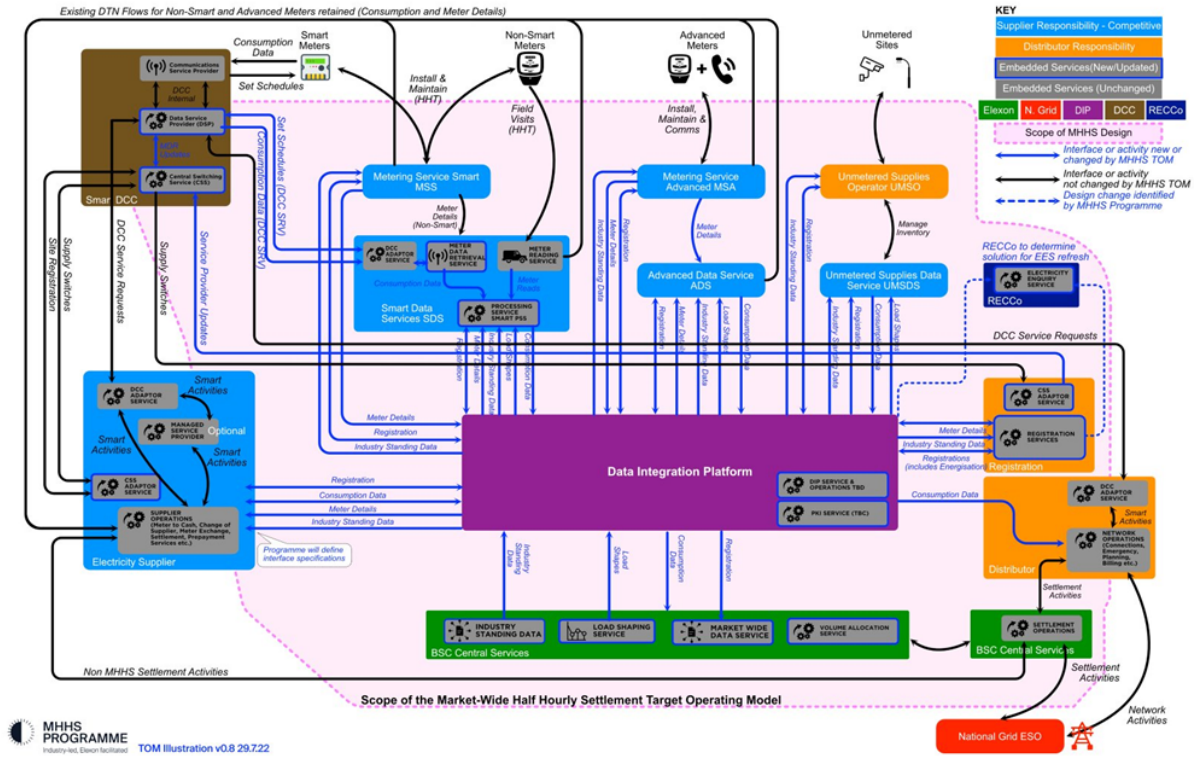
Knowledge Management

- Most Viewed Knowledge Articles
- Knowledge Article Usage by Category
- Knowledge Articles with Negative Feedback
- Knowledge Base Article Aging (Time Published)

Service Level Management

- SLA Breach Trends by Assignment Group
- Open Tasks with SLA Breaches
- SLA Achievement Rate
- SLAs Met or Breached by Priority

18.7 MHHS Target Operating Model



18.8 3rd Party SLA, Service Hours and Contact Details

At the time of issuing this version of the Service User Operating Manual, the 3rd Party SLA, Service Hours and Contact Details list is not yet available. These details are currently being collected through Elexon-led workshops and information gathered via webforms

18.9 Post Major Incident Review Template

ELEXON

Post Incident Review

Incident Details

Incident Title	
Incident Ref	
Incident Report Ref	
Service Affected	
Date/Time Service Impacted	
Date/Time Service Restored	
Major Incident Manger(s)	

Incident Description

Business Impact

Incident Summary & Action Performed

Incident Resolution

Affected Services (Please list all affected services)

ELEXON

Affected Users (Please provide an estimate of the number and groups of users impacted)

Major Activities and Timeline of Events

Please describe the major activities and their associated timestamps during the incident

Date & Time	Event	Comments

Root Cause Analysis

Root Cause (if known)

(If the root cause is not yet known, please provide the current status of the investigation)

Follow-up Actions

Please list any follow-up actions that have been identified as a result of this incident review

Owner	Action	Due

Process Review

Please provide a brief evaluation of the coordination and list any areas of improvement in the execution of the Major Incident Process

Additional Notes

Please provide any additional information or insights related to this incident

18.10 FAQ's

Question	Answer
What should I do if I haven't received a notification from the Service Desk after 15 minutes	Call the Service Desk on 03700 106950 to report the lack of notification

18.11 ServiceNow – Cases, Incidents & Comms

Case

A Case is a record that represents a customer request, inquiry, or issue. It is used to track interactions between a customer and the support team, ensuring that the request is properly addressed and resolved.

The Case stays with the Service Desk and the Service Desk are responsible for managing the communication with the customer

Incident

An Incident is an unplanned interruption or degradation of a service that needs immediate attention and resolution. They are created from a Case and are designed for the Technical Team to work on the issues, Incidents can be passed to different resolver groups

Communications

There are 4 different methods of communication:

ServiceNow Updates

These are manually updated within the Case from Customer Visible Comments, the Service User will then receive an email with a link to the Service Portal allowing the Service User to see the update

- The Service Portal is not updated directly, the ServiceNow Case is
- Customer Visible Comments are deigned to remove any technical communication between resolver teams
- Updates are made manually to allow for checking for suitability and if necessary, removal of technical or sensitive information

Major Incident Comms

Sent out via a ServiceNow Email group that provides business and impact language updates on the progress and resolution of a Major Incident

BSC Website Update

The BSC website is updated with the progress and resolution of a Major Incident, subscribers to the BSC website will receive the updates

Industry Circular

These are updates issued to Market Participants regarding issues related to IT systems or infrastructure