

Salesforce Response to Ofgem Consultation: Smart Secure Electricity Systems – Implementing the Load Control Licensing Regime

Salesforce Response to Ofgem Consultation: Smart Secure Electricity Systems – Implementing the Load Control Licensing Regime

Executive Summary	3
Part 1: Responses to Smart Secure Electricity Systems: Implementing the load control licensing regime (Main Consultation)	5
Part 2: Responses to Annex C: Draft load control licence application form	12
Part 3: Responses to Annex D: Draft load control consumer protection guidance	13
Appendix 1: Glossary of Terms and References	14

Mark Gilbey

Salesforce, Industry Advisor

mgilbey@salesforce.com

+44 (0) 7535 085 347

Ronald Starreveld

Salesforce, Distinguished Enterprise Architect

rstarreveld@salesforce.com

+ 44 (0) 7826 875 703

This response represents Salesforce's views as of February 2026. Our positions and capabilities may evolve over time. The information provided is for informational purposes only.

Executive Summary

Salesforce welcomes Ofgem's consultation on the implementation of the load control licensing regime. We recognise that the transition from unregulated flexibility pilots to a licensed, critical infrastructure service is a fundamental shift for the energy sector. The introduction of the requirement to hold a licence to undertake load control activity by 2027 is a necessary step to ensure consumer protection, cyber security, and grid stability.

Prospective licensees face a significant new administrative burden. To operate lawfully, they must demonstrate rigorous adherence to Annex C evidence requirements and Annex D consumer protection guidance. The final solution must be more than a technology platform and should be designed as a Licensee Operating System. This should provide the Compliance and Trust Layer that enables organisations to manage the application process, automate monitoring, and operationalise consumer protection at scale.

While Salesforce strongly supports the Licence Policy Principles (Consumer Protection, Energy Security, Vibrant Markets), our response highlights specific operational risks that should be addressed to ensure the framework is successful and scalable:

- **Alignment of Timelines and Standards (Q4).** We support the 12-month transition period only on the condition that it commences after the Tier 2 CAF (Cyber Assessment Framework) Profile is finalised. Licensees cannot be expected to architect compliant systems against undefined security standards.
- **Data Standards over Manual Reporting (Q14).** We challenge the reliance on manual quarterly RFIs and spreadsheets. To minimise regulatory burden and enable Compliance by Design, we urge Ofgem to publish a Standardised Data Taxonomy and API Schema immediately. This will allow licensees to automate reporting directly from their CRM platforms to the regulator.
- **Independent Governance (Q23).** We raise concerns regarding the proposed role of the industry-led Security Governance Group (SGG) in assessing licence applications. To protect Intellectual Property and prevent conflicts of interest, sensitive cyber security assessments should be conducted by independent auditors or Ofgem, rather than industry peers.
- **Objective Suitability Checks (Annex D).** We advise against the requirement for licensees to assess subjective criteria such as a consumer's money-management skills. This is operationally unfeasible and intrusive. We recommend replacing this with Objective Indicators (e.g., payment history, Priority Services Register status) that can be validated systematically within a CRM.

Salesforce is committed to supporting Ofgem and the industry in delivering a secure, flexible energy system. By adopting a platform-led approach to regulation, Ofgem can foster



a vibrant market where compliance is automated, consumers are protected by design, and innovation can thrive.

Part 1: Responses to Smart Secure Electricity Systems: Implementing the load control licensing regime (Main Consultation)

Q1. Do you agree that the Licence Policy Principles, as well as Ofgem's Growth Duty, are the correct principles to guide the development of Ofgem's implementation proposals?

Agree. We support the balance between Consumer protection and Enable vibrant markets. To achieve this without stifling innovation, the market requires scalable digital infrastructure. A unified platform that standardises consumer protection workflows (Principle 1) while automating the administrative burden to support vibrant markets (Principle 3).

Q2. Are there other measures Ofgem and DESNZ should consider in order to ensure the regime is proportionate and our approach minimises unnecessary burden?

Yes, Ofgem should explicitly encourage Compliance by Design through digital platforms. Minimising burden requires moving away from manual spreadsheet reporting to API-led regulatory reporting. By integrating operational data directly into a CRM that leverages AI and Agents to deal with the complexity and scale of the distributed energy market, licensees can generate compliance reports automatically, significantly reducing administrative overhead.

Q3. Do you agree with the proposed application form evidence requirements for each area?

Agree. The requirements for Operational capability and Consumer protection obligations are critical. Prospective licensees can demonstrate capability by using a CRM as their system of record showing that consumer consent, vulnerability data, and complaint logs are managed in a secure, auditable cloud platform provides strong evidence of capability from Day 1.

Q4. Do you agree with the proposal for a 12-month transition period?

Conditionally agree. We support a 12-month window, provided it only commences once the Tier 2 CAF Profile is published in final form. Starting the clock before the technical

standard is defined creates unacceptable regulatory risk for operators attempting to build 'Compliance by Design' systems.

Q5. Do you agree with our proposed application process for certain licensed suppliers?

Agree. Avoiding duplication for suppliers already subject to rigorous conditions is proportionate. For suppliers already using a CRM platform, the dual track is seamless, allowing them to extend their existing data model to include Load Control permissions without re-platforming.

Q6. Do you agree that the proposed application process for certain licensed suppliers should apply to licensed domestic suppliers, and not licensed suppliers who supply non-domestic customers only?

Agree. Non-domestic suppliers are not subject to the same strict consumer protection regimes required for domestic flexibility. The solution should allow licensees to segment customers (Domestic vs. Non-Domestic) and apply different logic and protection workflows to each, ensuring that the rigorous consumer protection logic is applied specifically where required by the domestic licence.

Q7. Do you agree with our proposed application process for non-licensed suppliers?

Agree. New entrants must prove they are fit and proper and financially responsible. For non-suppliers, adopting an industry-standard framework for financial and management controls demonstrates to Ofgem that the new entrant has a robust system to manage customer data, reducing the perceived risk of the application.

Q8. Do you agree that the proposed application process for different types of applicants is proportionate and reflects the SSES purpose and Licence Policy Principles?

Agree. It appropriately scales the evidence burden based on existing regulatory oversight. A small new entrant can use a standard platform to meet basic requirements, while large Dual Licensees can use complex, integrated instances to manage millions of assets.

Q9. Do you agree that our proposed timelines for licence application processing are reasonable?

Agree. The 9-month assessment window aligns with supply licence standards. To ensure processing falls within these timelines, applicants should use the platform to manage their side of the application, ensuring all evidence requirements are tracked, version-controlled, and submitted completely, reducing back-and-forth delays.

Q10. Do you agree with our proposal that tacit authorisation should not apply to the load control licence?

Agree. Given the risks to cyber security and grid stability, active authorisation is essential. Tacit authorisation implies a lack of scrutiny. We encourage active scrutiny; the platform generates the audit trails required to proactively prove compliance, removing the desire for passive authorisation.

Q11. Should Ofgem reconsider the question of tacit authorisation in future?

Only once the market is mature and risks are fully understood.

Q12. Do you agree with the proposed approach to compliance-related monitoring?

Agree. We support the focus on Complaints and Alternative Dispute Resolution and Financial Responsibility. The complaints handling solution platform should create a timestamped audit trail of every interaction, enabling licensees to effortlessly respond to Quarterly RFIs on complaints type and volume.

Q13. Do you agree with the proposed approach to market insights-focused monitoring, and are there any additional market indicators we should consider tracking?

Agree. Tracking FSP customers, Tariff data, and Switching data is vital. The solution platform should ingest operational data (e.g., number of devices controlled) and combine it with commercial data (tariff types) to produce these market insight reports automatically, ensuring Ofgem receives accurate, real-time views of the market.

Q14. Are the proposed RFIs proportionate and manageable?

Disagree, unless standardised. Frequency is not the issue; format is. Quarterly RFIs are only proportionate if Ofgem publishes a fixed Data Taxonomy/API Schema at launch. Without a fixed digital schema, these requests effectively mandate manual labour, contradicting the principle of minimising regulatory burden.

Q15. Please estimate the costs for your organisation for responding to the proposed RFIs.

While the government estimates costs between £7,000 and £24,000 per annum, we believe that for organisations using a platform that utilises AI with a robust and integrated data model, these costs will be at the lower end. Automation and AI removes manual data gathering, ensuring that responding to RFIs is a "click-to-report" activity rather than a manual project.

Q16. Do you agree with our proposed risk-based and proportionate approach to compliance under the load control licensing regime?

Agree. Focusing on Treating customers fairly and Cyber security as priority areas is correct. The solution platform should risk-rate their own customer base. For example, identifying vulnerable customers (Priority Services Register) ensures that compliance resources are focused on preventing harm to those most at risk, aligning with Ofgem's risk-based approach.

Q17. Are there additional factors we should consider when determining the level of compliance engagement for different types of licensees?

Ofgem should consider the digital maturity of the licensee. Licensees using certified, auditable platforms should be recognised as having lower operational risk than those using spreadsheets or bespoke, unverified legacy systems.

Q18. Do you support the proposal to use informal account management relationships to support licensees into compliance in the early years?

Agree. This collaborative approach fosters a Compliance by Design culture. It facilitates this relationship by allowing licensees to share dashboards or specific reports directly with

Ofgem account managers, creating a transparent, single source of truth for compliance discussions.

Q19. Do you agree with the proposed priority areas for compliance engagement?

Agree. Cyber security, treating customers fairly and operational controls are the correct priorities.

Q20. Do you agree with our proposal to align enforcement under the load control licensing regime with Ofgem's existing enforcement approach?

Agree. Consistency reduces uncertainty. The solution platform should provide the forensic data required during an enforcement investigation. If Ofgem investigates a breach, the platform should provide the immutable logs of who did what and when, facilitating a swift resolution.

Q21. Do you agree with our proposed enforcement approach for multiple licence holders?

Agree. A coordinated approach prevents double jeopardy. A single customer view that spans both supply and FSP licences. This ensures that if a compliance issue arises, the licensee can instantly see if it impacts one or both licensable activities.

Q22. Are the regulatory requirements for different types of Load Controller sufficiently clear?

Agree. The distinction between <300MW and >300MW (OES) is clear. Regardless of size, the solution platform should provide a security posture that scales. Whether a licensee is small (<300MW) or a critical OES (>300MW), the underlying customer data resides on the same zero-trust architecture.

Q23. Are the regulatory requirements for different types of Load Controller sufficiently clear?

Agree with the standard, Disagree with the assessor. While we support the CAF standard, we object to 'industry-led' bodies assessing licence applications. To protect Intellectual Property and prevent anti-competitive behaviour, cyber assessments involving sensitive

infrastructure data should be conducted solely by Ofgem or independent auditors, not market participants.

Q24. Do you agree with the proposed approach to cyber security monitoring and compliance?

Agree. Continuous monitoring should be a feature of the solution platform. It allows licensees to proactively detect threats to customer data, satisfying the requirement for ongoing vigilance.

Q25. What would you suggest is a reasonable equivalent of a CRA Audit?

Industry standards such as ISO 27001 or SOC2 Type II reports should be considered reasonable equivalents.

Q26. Do you agree with the inspection process outlined for the cyber security of below 300MW Load Controllers?

Agree. Ofgem must have the power to inspect premises and systems. In a cloud-first world, inspection often means reviewing digital logs to provide auditors with restricted access to review security settings and access logs without compromising live customer data.

Q27. Do you agree with our proposed approach to licence modifications?

Agree. As licence conditions evolve, low-code architecture allows licensees to rapidly modify workflows (e.g., changing a consent script) to remain compliant with new modifications without expensive re-coding.

Q28. Do you agree with our proposed process for the transfer of a load control licence?

Agree. Transferring a licence involves transferring data. The data portability tools ensure that if a business is sold, consumer records and consent histories can be securely transferred to the new entity in compliance with GDPR and licence conditions.

Q29. Do you agree with our proposed approach to extending/restricting a licence?

Agree. If an FSP wishes to extend to become a Load Controller, they should simply turn on additional modules within the solution platform to handle the new data requirements, supporting business scalability

Q30. Do you agree with our proposed approach to revocation of the load control licence, including our proposal to include a revocation item on the basis of failure to comply with the NIS regulations?

Agree. A failure in NIS compliance suggests a fundamental risk to the Energy Security principle. This underscores the need for a secure foundation, which mitigates the risk of NIS non-compliance related to data systems, thereby protecting the organisation from licence revocation.

Q31. Do you agree with our proposed approach to cost recovery for the load control licensing regime?

Agree. While the levy covers Ofgem's costs, the licensee's internal costs are best managed through efficiency. Investing in the right solution platform ensures that the operational cost of maintaining the licence remains low, preserving margin in this low-margin/high-volume market.

Part 2: Responses to Annex C: Draft load control licence application form

Q1. Do you consider the information and evidence requirements in the draft application form to be clear and aligned with the policy intent?

The requirements, specifically in Tier 1, are well-structured.

- **Section 19** (Operational Capability): The requirement to provide a plan for the first two years' operation is aligned with ensuring market stability.
- **Section 20** (Consumer Protection): The request for a statement of intent regarding SLC 11-14 is clear. It forces applicants to proactively consider how they will handle exit fees and mis-selling before entering the market.

Q2. Do you have any comments on the overall usability and structure of the draft application form?

The structure is logical. The separation of Tier 1 (standard info) and Tier 2 (additional info on request), is efficient and prevents applicants from having to submit excessive documentation unless specifically requested for scrutiny.

Part 3: Responses to Annex D: Draft load control consumer protection guidance

Q1. Does the guidance contain enough information to support you in complying with the consumer protection conditions?

We welcome the detailed framework, particularly the clear data requirements in Table 3 (Suitability) and Table 7 (Exit Fees). However, we strongly advise against the requirement in Table 3 to assess a customer's money-management skills. This criterion is subjective, intrusive, and difficult to standardise across different agents. It also requires manual intervention, preventing the automation necessary to scale flexibility services efficiently.

Recommendation: We recommend Ofgem amends the guidance to focus on objective indicators (e.g. payment history, Priority Services Register status) rather than subjective skills. Objective data can be securely processed within a CRM to enable compliance by design, ensuring consistent, audit ready suitability checks without invasive questioning.

Q2. Are there any additional risks that are not currently addressed by this guidance?

The guidance covers the primary risks well. However, we suggest further emphasis on interoperability risks mentioned in paragraph 3.8. As consumers stack multiple services, the guidance could provide more examples on how FSPs should communicate exclusivity clauses or technical conflicts to consumers to avoid confusion.

Appendix 1: Glossary of Terms and References

Term	Definition	Source Alignment
CAF	Cyber Assessment Framework: The standard for security self-assessment	Defined in Consultation Question 23
CRA	Competent Region Audit: An audit requirement for cyber security	Defined in Consultation Question 25
FSP	Flexibility Service Provider: Entities managing load control	Defined throughout Consultation
NIS	Network and Information Systems: Regulations concerning cyber security	Defined in Consultation Question 30
OES	Operators of Essential Services: Licensees >300MW	Defined in Consultation Question 22
RFI	Request for Information: Quarterly data requests from Ofgem	Defined in Consultation Question 14