POL00447765

Post Office Limited
Finsbury Dials
20 Finsbury Street
London
EC2Y 9AQ

Dr. Vikas Shah
Chair of Audit, Risk and Assurance Committee
Department for Business, Energy and Industrial Strategy

By way of email GRO

19 December 2022

Dear Dr. Shah,

Deteriorating Risk Profile of Post Office

We have appreciated your interest in our developing risk profile and governance. There are some difficult external events, from RMG strikes to our need to replace Horizon, that are increasing our risk profile and creating additional financial pressures. We are having to reduce risk mitigation as a result. Our ARC therefore wanted to give you a heads up on some key risk areas that are now outside tolerance.

The following risk areas are expected to remain outside of tolerance until the funding position improves:

1. **Loss of Availability of critical systems (Cyber Risk)** : Due to external malicious actors, there is a risk that the Post Office critical systems become unavailable. Reduced funding will prevent Post Office from improving its maturity of Cyber Security controls over the next 3 years. Whilst we have implemented multifactor authentication to strengthen our cyber defences and are currently reviewing responses to ransomware attacks, the residual risk position and exposure to cyber threat remains unacceptably high.
2. **Inability to extend Fujitsu Contract:** The Fujitsu contract is currently being managed within the extended contract agreement. The contract is due to cease in March 2025, by which point the New Branch IT system (NBIT) must be fully operational. The ability to extend the contract may be required as contingency for any delays with NBIT and also to ensure a continuation of service for end of life items and datacentre lease arrangements. It is unclear if we will be able to negotiate an extension to the agreement. Furthermore, if an extension can be negotiated, there will be increased costs, for which funding is currently not available.
3. **Poor management of unstructured information** : There is a risk that we do not have adequate oversight of information held within physical and digital locations, which could lead to the inability to locate and retrieve information when required, as well as non-compliance with legislation such as the Data Protection Act, resulting in financial, regulatory and reputational harm. A programme was stood up to address shortcomings in Post Office's data governance and management, however, the scope of this work was significantly curtailed due to reduced funding allocation. Whilst we will make slow progress in reducing the risk, it is likely that the risk will remain outside of tolerance over the next 3 years.

POL00447765

We have implemented enhanced monitoring to manage the above risks, as well as other areas of concern, which are outside of appetite or tolerance. These include:

- **Inadequate Service Resilience:** Without appropriate contractual resilience tests with our suppliers, there is a risk that following a catastrophic IT incident, disaster recovery cannot be invoked.
- **Overturned Historical Convictions** : Potential for civil actions from claimants.
- **Regulatory:** Post Office operating model may not be supportive or agile to accommodate changing regulatory and control landscapes.
- **Postmaster Proposition:** The risk that Post Office's retail value proposition is not profitable enough to sustain Postmasters' business.
- **Non-compliance with IR35:** Post Office is changing its approach to bring more contractors inside IR35. However, it is unclear to what extent HMRC may rule with regards to our historical practices.

Happy to discuss or welcome you at a future Post Office Audit, Risk and Compliance meeting.

Kind regards,

Carla Stent

Chair of Post Office ARC