POL00031409

Zebra Action Summary

Document Control

1 Overview

Author:	James Rees		
Reviewer:	Emma McGinn		
Review and Sign-off:	Julie George		
Version:	0.3	Date:	12 June 2014

2 Revision History

Version	Date	Author	Changes
v0.1	5 June 2014	James Rees	First Draft
V0.2	10 June 2014	Emma McGinn	Reviewed
V0.3	12 June 2014	Julie George	Draft review and sign-off

POL00031409

1 Introduction

This document is in response to the Zebra review and highlights specific areas regarding the Horizon solution, outlined in Deloitte's report, with suggested controls Post Office could implement to mitigate the areas the project highlighted.

2 Scope

The scope of this document is those areas covered in the Zebra report only and does not include any other areas outside the scope of that report.

3 Zebra – Overview

Deloitte's Zebra report has outlined a number of areas relating to the Horizon solution requiring remediation and/or changes in order to protect and maintain the integrity of Horizon on an ongoing basis. These would provide a greater level of support and assurance of the Horizon platform through Fujitsu as the service provider, Post Office as the customer and, potentially, Atos as a key service provider for the IT governance service.

Other areas of the Horizon solution highlighted in the report that require further investigation and remediation are the audit and risk management aspects together with the oversight and governance of the Horizon solution.

4 Zebra – Remediation Items

Below are the recommendations for the remediation of the items outlined in the Zebra report as well as the board summary report:

4.1 Governance

There were a number of governance items outlined as failings in the report that need to be addressed and recommendations pertinent to these items are as follows:

4.1.1 Horizon Management Council

Since Horizon is a critical business function of the Post Office estate a management council should be created in order to ensure the ongoing oversight, management and support of this business critical infrastructure going forward, this is in addition to the current Information Security Management Forum.

Risks and issues relating to the Horizon solution of a high or critical nature should be flagged to this group who will then review them and take appropriate action to maintain the integrity of this business critical asset.

POL00031409

Recommended remediation:
Creation of a Horizon Management Council made up of one representative from each organisation (Post Office, Atos and Fujitsu). This council may have additional memberships but no more than 6 primary council members should be appointed. Any other individuals required should be brought in as ADVISORY members only when specialist advisory skills are required, and do not have a say in the management of the solution, this is the province of the primary members.

This group should meet quarterly, as a minimum, or after any significant change or issue.

It is further recommended that a similar Management Council should be set up for all critical business functions.

4.1.2 Documentation update and ongoing Maintenance

Current, accurate and auditable documentation is imperative to the management of a critical business asset such as Horizon.

One significant failing outlined throughout the main report was the lack of information available to Deloitte when reviewing Horizon, including process, procedure and governance documents, and this should be resolved as soon as possible.

Recommended remediation:
A complete document pack to be created that outlines at least the following items:

- Policies
- Procedures
- Standards
- Development roadmap
- Solution overviews
- Solution diagrams
- Risk register
- Detailed solution documentation (technical)
- Business continuity

This document pack would need to be centrally owned, managed and maintained and would possibly also include information regarding how Horizon handles accounting and financial information.

4.1.3 Change Control

A number of items outlined in the report related to the lack of an effective governance process for recording and maintaining changes to the Horizon infrastructure. This was a common theme throughout the report and is an item high on the list for resolution within Post Office (ISAG), Atos and Fujitsu.

POL00031409

A single change control process covering all the pertinent points will efficiently and effectively track changes that occur in that environment from a technical and development viewpoint. This will, in turn, need to include the updating of the Horizon infrastructure documentation as part of the process as the documentation was highlighted in the report as failing.

Recommended remediation:
The creation of a process for recording, authorising, testing and implementing all changes within the Horizon solution which is both effective and ensures that all appropriate parties are informed as changes occur.

The change control process needs to be both effective and support the reporting function to track how Horizon has evolved over time, track the risks and the critical business assets as well as allowing a far greater understanding of the solution and what is required to secure it.

This should be the responsibility of all three organisations (Post Office, Atos and Fujitsu) and all should support that process.

4.1.4 Financial Reviews

One of the main concerns within the Deloitte report is the balancing of financial accounts and the potential for errors should certain technical issues arise. Technical issues and connectivity issues will always be a risk within any technical environment and it is strongly advised that a program is put in place to undertake auditable controls, ongoing training, spot checks and regular reviews from Post Office's Audit department to make sure that errors in processing are kept to a minimum, and quickly identified.

Recommended remediation:
The creation of an audit program by Post Office's Finance department in order to review samples of data from sub-postmasters. This would ensure consistency of accounts and enable a higher chance of detecting errors in accounts due to problems with Horizon.

Reports should be generated after each audit and used to improve the Horizon product, as well as provide auditable records of assurance; this should feed into the Horizon Management Council for considered remediation.

Workshops should be undertaken on the financial accounting aspects of Horizon, with appropriate controls introduced as determined by the resultant gap analysis exercise and training in support of the controls and system.

4.1.5 Risk Assessment

The Deloitte report advised that Horizon should undergo a full risk assessment to highlight the key assets that comprise the

POL00031409

Horizon solution, including the risks associated with those assets. This should be undertaken exclusively by Information Security professionals together with key Fujitsu staff.

Recommended remediation:
Undertake a full risk profiling and assessment in order to identify the key assets and risks associated with those assets that make up the Horizon solution. This would include full oversight of Fujitsu's Horizon risk management documentation that should have been undertaken as part of the PCI DSS and ISO27001 Information Security requirements.

The risk assessment information gathered from this process should be updated regularly and feed into the change control process (as well as the change control process feeding into the risk management process) to ensure that a greater level of security oversight and involvement is promoted.

Horizon is a critical business asset to the Post Office and, as such, risks to this environment need to be clearly understood and treated.

POL00031409

4.1.6 IT Assurance

Deloitte highlighted in the report that there was a lack of assurance in the technical oversight of the Horizon solution throughout the Horizon lifetime. This was quite specific to traceability as well as the tracking of changes and oversight into future development.

Recommended remediation:

A Post Office IT Assurance function needs to have regular reviews and updates with key Fujitsu staff, as with all critical business systems, ensuring that the Horizon platform is carefully developed in line with ever changing business needs. This should to be driven by the Post Office business process, be a function separate from operational IT Services and with oversight from the Horizon Management Council.

It is strongly advised that, in the long term, a roadmap is developed to outline expected changes and improvements to Horizon, these may already be in place and, if so, need to be carefully released in order for the risk assessment and management to be effective.

4.2 Technical

There were a number of technical items outlined as failings in the report that need to be addressed; recommendations pertinent to these issues are as follows:

4.2.1 Data Retention

The report outlined that data is held within Horizon for seven years, which is in line with the UK retention period legal requirements, though the report infers that this may not be enough in some cases.

Recommended remediation:

The retention periods should be carefully reviewed by Data Protection professionals and key business departments that own this data, preferably with oversight from the Finance department. If longer retention periods are required then this needs to be defined both from a governance and technical perspective.

There are numerous technical possibilities to cater for this, but this should be defined once retention periods have been agreed.

4.2.2 Data Logging

One point raised in the report was that it was possible for someone with privileged access to delete data from specific areas of Horizon. This is always a risk with individuals using admin or power user accounts and is a persistent risk, one that needs to be catered for in almost any organisation.

Due to the sensitive nature of the information contained in the databases, monitoring of those databases should be put in

POL00031409

place using technology to detect and record deletions and administrative changes to the databases. If possible, alerts should also be generated for mass deletions and high level risk changes to database schemas.

Recommended remediation:
The solution currently in place may be able to undertake the level of logging required within the Horizon solution. It is recommended that the current logging and logs are reviewed on a daily basis.

This needs to be investigated further and the options on how to handle this defined through the risk management process and based on the solutions already in place or ones that could be procured to handle this.