

Group Assurance

BSFF Update 20 December 2023



Content

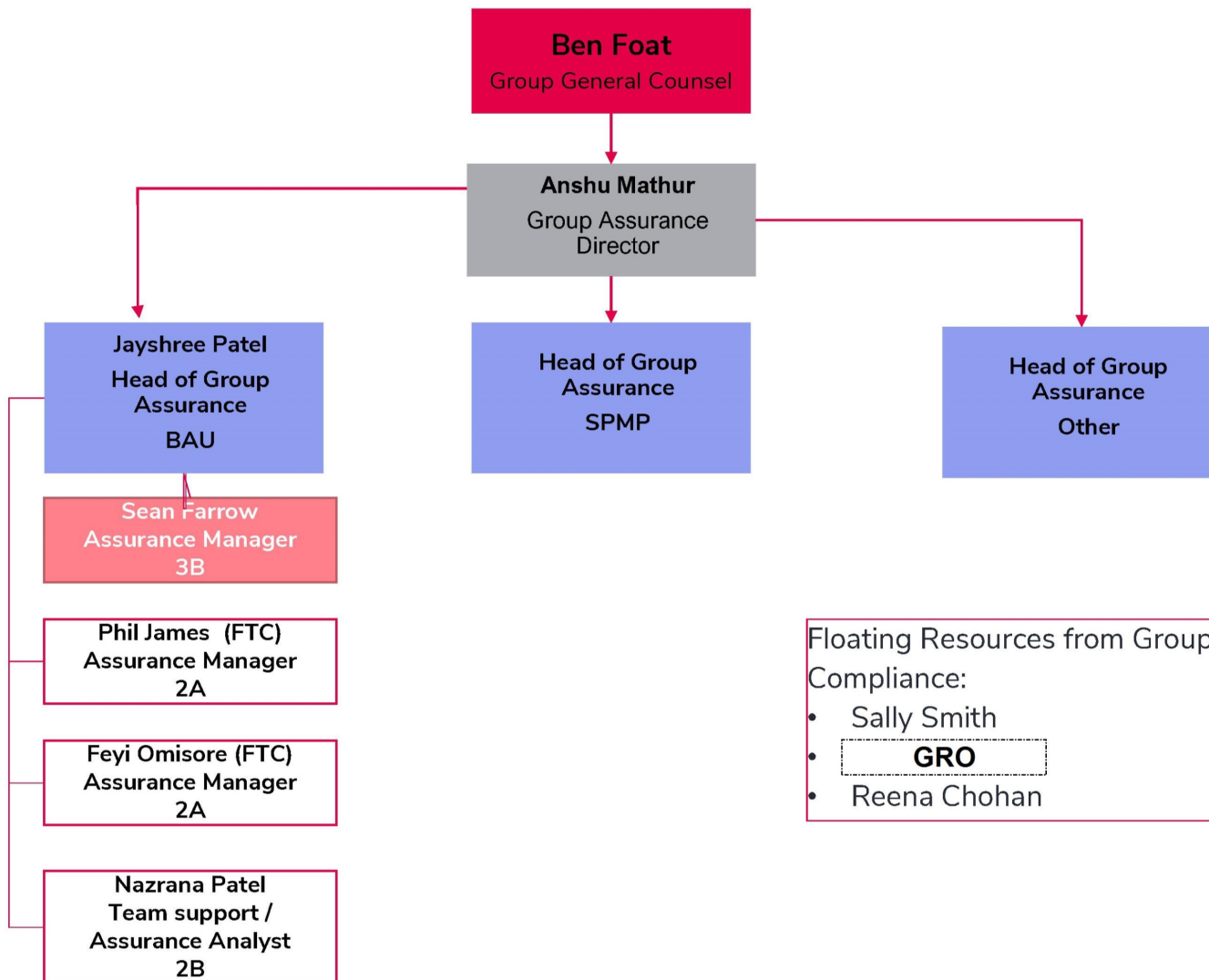
- Assurance Team Structure
- Assurance Activities on a page
- Common Issue Judgement
- PM support Policies
- Horizon Issue Judgement
- Speak Up and CIU
- Other Reviews
- Action Tracking and Integrated Assurance
- SPMP Assurance
- Retail Assurance

It will be important for POL to demonstrate to the Inquiry that measures have been put in place to prevent the same issues being repeated as well as what it is doing by way of continual monitoring and improvement.

It is recognised that there is cross over between some of the topics.

and consider what evidence they might request if they were in the Inquiry's shoes.

- a) what improvements have been made across POL from 2000 – to date,
- b) anything further that POL has put in place or intends to put in place going forwards.
- c) how POL is or proposes to ensure continual monitoring of these areas to ensure that history does not repeat itself and to test how effective the change(s) have been.
- d) the commitments it has made to learn lessons and make changes
- e) the work undertaken by POL to date, further work that is required in each area and identify documents that may assist in drafting narrative documents.



Member of:

- Inquiry Steering Committee (ISC)
- IDG 2.0

Regular attendee of:

- RCC
- ARC

Assurance activities overseen by:

- RCC
- ARC

Floating Resources from Group Compliance:

- Sally Smith
- **GRO**
- Reena Chohan

Assurance Activities on a page

Group Assurance - Activities on a Page and outcomes

Control Framework

PO Control Framework

- Framework includes 3 LoD and RACI between 1st line, 2nd line and 3rd line.
- Defined / Clarity for key risks and controls
- Guidance for – Control Evidence, control sampling – first and second line.
- **Submitted and approved as Draft at Sept 2022 ARC**

Tech (Change)

Assessment of Tech controls

Speak Up / Whistleblowing

Assessing the effectiveness and adherence of processes and controls for Speak up cases

Central Investigations

Assessing the effectiveness and adherence to processes and controls for Investigations

Status / Outcomes

PO Control Framework

- The PO Control Framework **remains in draft.**
- Principle are applied on best endeavours basis, and via all Assurance reviews

Tech (Change)

Complete - BAU

Speak Up / Whistleblowing

Complete - Satisfactory

Central Investigations

Complete - Needs Significant Improvement

Group Assurance - Legacy Activities

Common Issues Judgement	Actions taken by POL in response to the Common Issues Judgement
Postmaster Support Policies	Assurance of effectiveness of Postmaster Support Policies
Inquiry Rule 9 Requests	Processes and procedures for dealing with Rule 9 requests from Inquiry
Horizon Issues Judgement	Actions taken by POL in response to the Horizon Issues Judgement
Historical Shortfall Scheme	Claims from current and ex-postmasters in relation to losses occurred due to shortfalls
Stamps Scheme	Claims from current and ex-postmasters in relation to losses occurred due to Stamp Stock
Suspension Payments	To obtain objective assurance of the Suspension Payment process – accuracy and completeness
Pause Payments	Provide assurance to HM Legal on their assessment of the risk of continuing to receive payments from Postmasters
NBiT business requirements	Identifying and ensuring accuracy of business requirements
Overtaken Historical Convictions	Ongoing - Remediation scheme for postmasters who were wrongly convicted
Inquiry Rule 9 / Sect 21 Requests	Ongoing - Supporting updates to process flows for Rule9/Sect 21 requests

Status / Outcomes

Common Issues Judgement	Needs Significant Improvement
Postmaster Support Policies	Needs Significant Improvement
Inquiry Rule 9 Requests	Unsatisfactory
Horizon Issues Judgement	PAUSED
Historical Shortfall Scheme	Needs Significant Improvement
Stamps Scheme	Satisfactory
Suspension Payments	Unsatisfactory
Pause Payments	Unrated recommendation not to pursue the recovery
NBiT business requirements	Unrated – some significant improvement opportunities identified for R3

Common Issue Judgement

Common Issues Judgement

OBJECTIVE & APPROACH

- To review the status of actions implemented to address / remediate issues raised within the Common Issues Judgement.
- A critical approach applied to assess evidence from a sustainability perspective and identify further risks or areas of improvement from a POL and/or Postmaster lens to prevent detriment and ensure appropriate governance / oversight.

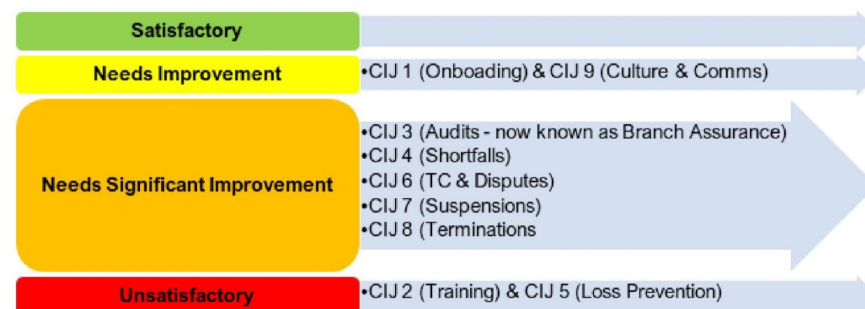
ASSURANCE OPINION

- A number of challenges had to be overcome and considerable time invested with the Retail team prior and during the review, this however has resulted in the following benefits for POL:
 - Single universe of actions (365)**, clearer ownership / risk articulation.
 - Central repository of evidence**, incl. links to sites, clearly tagged to CIJ:
 - 1,594** evidence items, and access to 53 live sites (containing policies, processes, documents, MI, and access to live systems such as Power BI Dashboards).
 - This **should** now be used for **continuous assurance and support Inquiry preparation**.

Retail have completed majority of the CIJ actions (97%). This in isolation is a considerable achievement, given the cost challenges, changes to personnel, team structures etc.

That said, and as mentioned above, our review has gone beyond the evidence, to review with a critical lens **whether the actions are sustainable, can demonstrate or track the impacts on PMs, and where applicable, there is appropriate oversight and governance.** With this context we have identified a number of significant improvement opportunities:

CIJ Action status – Assurance View	Number	% of total
Completed	269	97%
Not completed	8	3%
Excluded from Assurance scope (linked to HIJ)	4	1%
*365 less duplicates 86 = 279	279	



Common Issues Judgement – Key drivers of Assurance Opinion 1/3

- Some original actions have not been completed or partially completed, for example:
 - Loss Recovery process has not been implemented
 - Stock Auto Rem and Stock Auto Replenishment - due to lack of funding
 - Refresher training is partially completed.
 - Discrepancies from returned stock is partially complete
- Fundamental thematic themes emerge which either negate the impact of the actions completed or lead to ineffective oversight of these:
 - **MI, Dashboards and Reporting (thematic across all CIJ)**
 - Whilst the Retail Team have considerable data, MI and dashboards it is very challenging to assess (on an E2E basis) what the overall impact has been of the actions delivered for CIJ.
 - It is unclear how KRI's, KPI's and exceptions are tracked holistically or triggered for escalations to ensure timely visibility, and appropriate governance, for example, the Complaints Dashboard does not provide qualitative information particularly in relation to Branch Assurance Reviews and Transaction corrections, to indicate if postmasters are seeing a positive change on the ground or not or whether a positive impact in a process is not negated by any other process (E2E view).
 - The GE receive on a regular basis a CIJ dashboard, this in our opinion therefore requires a revamp and should be created with a E2E view of the PM journeys or akin to a balanced scorecard that many consumer facing organisations have to measure their impact and protection of consumers.
 - **Root Cause Analysis (thematic across all CIJ)**
 - Whilst causes or buckets of errors is captured for Transaction Corrections, root cause analysis is not currently used and or reported to support understanding of why issues/errors are occurring. We believe outcomes of this type of analysis could be used to improve training and support.

Common Issues Judgement – Key drivers of Assurance Opinion 2/3

- **Quality Assurance (QA)**

- QA processed are being used/introduced to various teams within Retail such as Branch Assurance and Transaction Corrections and Disputes, this is a positive step to provide assurance on activities completed by these teams. And should therefore be closely monitored to ensure these are embedded.
- Scripts have been introduced to ensure a consistent approach to contact with Postmasters, and a call recording system has been implemented allowing call monitoring to take place. However, in some instances, calls made via mobile phones cannot be recorded and therefore not able to be monitored.
- PM Suspension payments are calculated by Finance however these are not independently checked to ensure the accuracy and or completeness of the Remuneration components.

- **Loss Recovery and Investigations**

- Based on the current approach to loss recovery for losses that have been investigated and found to be genuine losses, POL is treating postmasters differently. Some Postmasters are not engaging with POL on losses and are not repaying them whilst other Postmasters who do engage with POL are repaying losses.
- Additionally, discrepancy cases identified following Branch Assurance reviews are not prioritised for investigation, not prioritising cases may mean the suspension time is extended unreasonably.

Common Issues Judgement – Key drivers of Assurance Opinion 3/3

- **Other Thematics**
 - A standardised approach to document control (incl. version control) needs to be adopted across the Retail team to ensure POL can demonstrate changes (or no changes) and evolutions to key processes and procedures.
 - Postmaster Support policies - this action has been picked up in CIJ areas where policies are mentioned, however overall, there needs to be a process or KPI's/metrics to assess the effectiveness and compliance to all Postmaster policies.
 - Effectiveness of Key Support roles
 - Conflicts in Decision making – Retail org design
- **Other Actions** - In addition to the Thematics, 29 additional actions were identified from the findings in each of the individual CIJ areas:
 - Onboarding – 2
 - Training – 6
 - Branch Assurance – 4
 - Central Ops – 8
 - Retail / Retail Ops – 8
 - Culture - 1
 - Postmaster policies - 45

Common Issues Judgement – Status of Assurance Actions

- Tracking, reporting and assessing status of actions formally commenced from December 2023.
- This is overseen via RCC and ARC.

STATUS @ 18/12/2023				Of the open actions:			
	Total actions raised	Closed	Open	Current	Due within 30 days	Overdue < 3 mths	Overdue > 3 mths
Common issues judgement	39	10	29	16	12	1	
Postmaster Policy Assurance reviews	45		45	45			

PM Support Policies

OBJECTIVE

Whilst there is a close alignment with CIJ reviews, and we have aligned both reviews where possible, the approach of the Postmaster policy reviews was fundamentally more myopic and did not apply a E2E view of the POL universe.

Outcomes

- [illegible]

Horizon Issue Judgement

HIJ – Assurance Review Paused

Row Owners	HIJ Actions	HIJ Lines	Review STATUS	Comments
Chris Leach	Build a robust capability to deliver change & prevent and manage defects in the future	3	In progress	<p>1. Key evidence still outstanding despite chasing (RG/CL) – MI on the number of defect post releases, and of which how many are PM impacting, Tally or MI of HSA decisions made categorized by #approved, #conditional approval, and # rejected, with a thematic of the drivers behind these articulated, universe for a) sub postmasters were not informed about identified defect b) some defects were not detected by automatic system checks and as a result lay undiscovered for years c) Legacy Horizon and HNG-X were not remotely robust as demonstrated by the number of defects found d)The lack of records or logs for the use of powerful access roles also contributes to this.</p> <p>2. Universe of defects still not sent. Horizon solution Authority processes and procedure are robust. That said improvements needed in capturing minutes, universe of change ie change can still bypass HAS.</p> <p>3. xxx</p>
Martin Godbold/Paul Smith	Understand and address the root cause of existing defects / Provide Sub postmasters with close to real time information on known defects in Post Office systems / Establish application monitoring processes and tools to proactively identify defects	5	In progress	<p>1. Underlying processes and procedures are adequate but need to be reviewed and refreshed with a PM lens / PM detriment lens. For eg Horizon Implementation Defect Review TOR, It is very difficult to assess efficacy of defect mgt process without an aggregated view of defects and their ageing, Test exit report – the so what is not clear from the report, basically, there is no formal summary of any risk assessment having taken place in this document, ie it cant be a standalone.</p> <p>2. Evidence collation not a priority. MG has taken over and consequently accountability is an issue.</p>
Dean Bessell	Build a robust capability to secure, control and audit access to Horizon / Provide an effective, transparent and auditable outcome for Postmasters in the event of financial discrepancies	7	In progress	<p>Feedback has been provided to DB, regarding sum of the parts vs how this come together from a universe, governance and monitoring perspective. Review feedback is being taken on board with revision being made and iteratively , albeit slowly, getting there. Refreshed data re-sent AM to review.</p> <p>All data sets or metrics may still not be generated. But great cooperation from CISO. TBC</p>
Sree Balachandran	Provide actionable information to Postmasters and POL to allow timely querying of transactions	4	Paused	<p>1. Evidenced received Nov. Very convoluted evidence, and in my opinion has been made complex.</p> <p>2. xxx</p>
Sally Rush/Paul Smith	Improve the Horizon Application to improve usability and reduce defects / Build a robust capability to manage data/Provide requirements to the data platform programme / Establish the capability to securely record and manage Transaction Corrections	15	Paused	<p>1. The way the journey has been laid out makes sense as it show the level of diligence applied to this area to identify problem statements (PS). That said:</p> <ul style="list-style-type: none"> The documents in many cases do not hang together to show the movement from PS to the number of issues that were finally targeted for remediation. (426 – 212 – 26 - ??) It is difficult to understand the impact POL has made vis a vis the HIJ areas/lines this is covering. A summary of actions taken, their impact, and how these are monitored would probably help. <ul style="list-style-type: none"> But with either linking to the PS or ignoring them. <p>le Overall this can be and should be simplified</p> <p>2. xxx</p>
Grand Total		34		

Speak Up and Complex Investigations Unit

Speak Up

GREEN - SATISFACTORY

OBJECTIVE

The objective of the review was to assess the level of Speak Up process compliance, when dealing with Speak Up cases.

SCOPE & APPROACH

- A sample of 10 Speak Up cases (raised between April 2022 – January 2023) were reviewed against Speak Up policies and procedures and focussing on:
 - Security and access of 'Speak Up' data – especially maintaining confidentiality/anonymity
 - Effectiveness of Speak Up communications
 - Speak Up monitoring and governance
 - Effectiveness of Speak Up training

Assurance Conclusion:

The Speak Up team was established approximately 18 months ago and during this period, the team have invested heavily in reviewing and updating processes and procedures and have also introduced monitoring dashboards for Speak Up which is reported to Group Executives and Board members monthly.

Whilst being a relatively new team, they are embedding robust processes and procedures, and have a culture of continuous improvement.

Consequently, our opinion is that the overall control environment is Satisfactory.

STATUS OF ACTIONS - 5

Four actions were closed as of 31st August 2023

One remains open –

"POL external Speak Up website is in the process of being changed and updated".

Work is progressing and forms part of the 2 year Speak Up strategy to raise awareness of the Speak Up function. The Speak Up team are working with the Comms team and have agreed a comms plan.

THEMATICS AND FINDINGS

1. Speak Up Process and procedures – Some improvement needed
2. Speak Up communications – No material exceptions Identified
3. Speak Up – Governance and first line assurance – No exceptions identified
4. Speak Up training – No exceptions identified

Complex Investigation Unit (CIU)

NEEDS SIGNIFICANT IMPROVEMENT

OBJECTIVE

The core objective of the review was to assess the level of process compliance in accordance with the Group Investigations and Co-operation with Law Enforcement Policy (GICLE) and the Investigators Manual.

SCOPE & APPROACH

- Our work sampled 8 investigations performed by the CIU team (over 2022 and 2023). For clarity this review excluded the CIU Assurance activities over Retail Investigations

Assurance Conclusion

The CIU team actively and constructively engaged with our assurance review, and they are overtly aware of the Common Issue Judgements.

Their intent and approach in ensuring mistakes of the past are not repeated can clearly be evidenced not only in their revised set of processes and procedures, but also in the positive behaviours and culture they are trying to embed within CIU and across POL.

Significant improvement reflects CIU to be able to **demonstrate adherence to their processes and procedures**, such as:

- Evidence to demonstrate **Head of CIU review, sign off or criteria for decision making has not been maintained** within CIU case files, for example, triage criteria, case closure, criminal investigation, conflicts etc.
- Meetings with CIU staff anecdotally show that **review meetings** are held twice a week on cases, these are not reflected in casefile9s).
- **Use and completion of key CIU documents need to be embedded consistently**, such as the Combined strategy/investigation strategy document and Investigation Control Document, or their non-use formally explained.
- **Case and file structures** have only recently been adopting a consistent approach therefore for older investigation (2022) navigating case files is challenging.

Group Assurance acknowledge that this is mainly due to the fact that the team is newly formed, with processes still being created and embedded, compounded by a heavy CIU workload.

STATUS OF ACTIONS

All actions closed as of 31st August 2023

Other Reviews

Inquiry (Rule 9)

OBJECTIVE

Assess POL's control environment, particularly relating to demonstration of adequacy and adherence to Rule 9 processes and procedures following receipt of Rule 9 requests from Inquiry

SCOPE & APPROACH

- 4 themes:- Disclosure and Data; Inquiry Readiness; Responsibilities (RACI); Witness Preparation
- Random sample of six Rule 9's selected for the period 9 August 2021 to 12 September 2022.
- Fieldwork was performed during three stages (December 2022-January 2023, February 2023 and June 2023) to ensure the Inquiry team could coordinate between various internal and external teams involved and that unhindered access to documentation to complete the review was provided.

OUTCOME

Documentary evidence to demonstrate compliance with processes and procedures could not be provided. Gaps related to application of POL governance and oversight, and assessment of completeness and accuracy.

Fundamental weaknesses in the control environment were identified such that management of key inherent risks and associated design and execution of controls was unsatisfactory.

Opinion - the risk of inaccuracy or omissions cannot be ruled out for Rule 9 requests covered in our sample period.

KEY THEMATICS AND FINDINGS

Based on the Rule 9 samples:

- Lack of clear consistency and governance around storage and traceability of documentation for Rule9 requests though their lifecycle
- Roles, Responsibilities and Ownership for Rule 9 process and governance were not clearly defined.

RED - UNSATISFACTORY

Suspension remediation review (at request of HM Director)

OBJECTIVE

Group Assurance have performed a review of Post Office's Suspension Remediation Review processes and procedures to assess the robustness of their control environment.

SCOPE & APPROACH

The Assurance Team performed a desk top review of the Historical Matters Suspension Payment Processes to identify key inherent risk and expected controls.

A sample of three Suspension Payments was then selected to perform a walkthrough to assess the effectiveness of controls.

This review was performed during June 2023, and therefore our opinions and comments reflect the state of the control environment during this period.

OUTCOME OF REVIEW

Our review identified that sufficient evidence does not exist to demonstrate whether key controls operating within the Historical Matters Suspension Payment team are being complied with.

There are significant gaps and weaknesses in the design of the Historical Matters Suspension Payment Processes whereby completeness, accuracy and or reasonableness of Suspension Payments cannot be assured.

STATUS OF ACTIONS

The status of the 10 actions identified at the time of fieldwork, are summarised below:

- Four resolved via Legacy team board paper
- Five changes to tightening the process completed
- One was already in place and being completed

THEMATICS AND FINDINGS

1. RACI and approvals process
2. Legacy and BAU approach consistency and calculation methodology
3. Document checking – bankruptcy, sanctions and ID checks
4. Legacy scheme cross checking process
5. QA on final correspondence to Postmasters

Pause Payments

OBJECTIVE

Objectively assess whether HM Legal's recommendation to continue to receive payments in connection to 21 PM cases deemed as low/medium was appropriate based on the evidence available.

APPROACH

Group Assurance reviewed a sample of six cases:

- two cases were randomly selected from the three categories - Apparent Dishonesty, Apparent NCE and CCJ.

All documentary evidence provided by HM Legal was reviewed for the six samples selected.

ASSURANCE OPINION

The process used by the HM Legal team to complete and document their assessment to continue recoveries of losses for 21 cases involving PMs is very methodical with good file structures and a clear application of logic to categorise the risk classifications.

That said our review has highlighted the following risks that management need to carefully consider prior to assessing whether recoveries should continue or be paused:

- It is unclear whether the POL individuals involved in these cases (audit, investigation, and security teams) and the processes and practices they adopted (dates range from 2006 to 2020) were similar to those that led to incorrect historical convictions.
- The level of documentation varied for the cases reviewed, in two cases (both CCJ) there was significantly less documentation.
- In cases where there was genuine theft perpetrated by third parties, it is unclear how POL discharged its duty of care to Postmasters. No evidence exists of POL employees advising the Postmasters to contact the police and/or check if they had Business insurance to cover such losses.

Consequently, in our opinion the associated risk in continuing to recover outstanding balances in relation to the 21 cases is extremely high, and the reputational risk outweighs the financial benefit.

Stamps (SS) & Historical Shortfall (HSS) Schemes

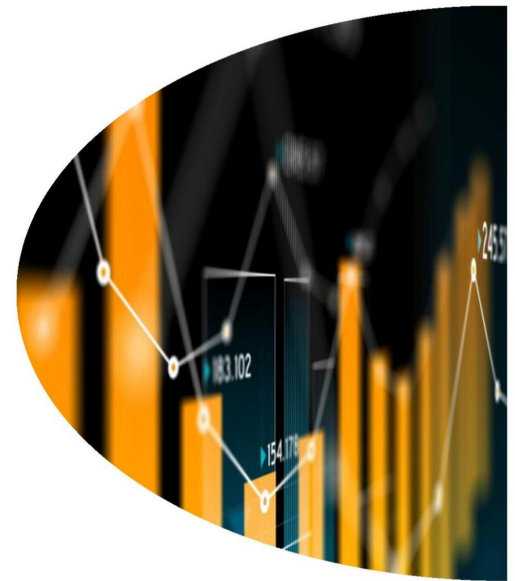
	Stamps Scheme	Shortfall Scheme
Objective	This review was completed following the closure of the Stamp Scheme, the objective was to ensure SS claims were dealt with in a fair and consistent manner.	This review was completed whilst claims were being assessed and the objective was to ensure the claims were dealt with in accordance with agreed processes.
Scope & Approach	The Review consisted of: <ul style="list-style-type: none">• review of 54 randomly selected SS claims; and• assessing responses to 67 Assurance questions along with evidence provided.	The Review consisted of: <ul style="list-style-type: none">• Assessing responses to 95 assurance questions including evidence; and• Review of 8 randomly selected claims.
Final Report Rating	As the Scheme was closed, and improvements made following initial and ongoing feedback, the report was not rated, however Minor improvements needs were identified.	Significant improvements were identified, and the report was graded Amber
Thematic actions	One key action was identified – a document retention policy had not been agreed, this has since been completed.	19 actions were identified across several themes including the HSS and Data universe, Document retention in Relativity, Governance (including oversight of 3 rd parties), Policies and procedures.
Action status	Action closed	All actions closed

Note – these were the first two schemes that were reviewed, and during the course of each review initial and ongoing feedback was provided to the relevant teams. As a result, the reviews took longer than anticipated however the learnings have been used to inform how future schemes are run.

Action Tracking and Integrated Assurance

Action Tracker

					Of the open actions:				
Review name	Function	Total actions raised	Closed	Open	Current	Due within 30 days	Overdue < 3 months	Overdue > 3 months	Report
Common issues judgement	Retail	39	10	29	16	12	1		Open
Postmaster Policy Assurance reviews	Retail	45		45	45				Open
Quality Assurance Framework	Retail	68	33	35	35				Open
A&CI	Multiple	7	3	4	4				Open
Speak Up	LCG	6	5	1			1		Open
Assurance and Complex Investigations (formerly CIU)	LCG	3	3						Closed
Stamp scheme	Remediation Unit	9	9						Closed
Historic Shortfall scheme	Remediation Unit	19	19						Closed
Suspension remediation review	Remediation Unit	10	10						Closed
Grand Total as at 18/12/23		206	92	114	100	12	2	0	



Integrated Assurance

Plans for integrated assurance

Following the completion of the Legacy assurance activities, Group Assurance is moving into the 'BAU Continuous Assurance' phase of the original plan.

Approach

Using our knowledge from the Legacy Assurance activities, Group Assurance has created an Assurance Universe which is made up of:

- CIJ activities
- Assurance & Complex Investigations
- Speak Up
- Remediation Unit

Each Universe has been shared with the business areas to gain feedback which has been collated into the final version. Workplans are now in the process of being created and shared.

Group Assurance is also supporting the Remediation Unit in completing ad-hoc Assurance activities.



SPMP Assurance



Why does SPM need an Integrated Assurance Universe?





What are the main areas of risk in the Integrated Assurance Universe?

The building blocks of the SPM Integrated Assurance Universe focus on those program or business activities that are fundamental to the go live of SPM, or those business functions that would be a consumer of SPM outputs. These are listed on the table to the right.

Whilst the ARC signed off on circa 10 areas we have gone beyond these to ensure all interdependencies are captured.

The universe once completed will remain a live, iterative artefact to ensure we capture new, emerging risk and lessons identified from assurance activities.

Ref	SPM/NBIT	Business Owner	Line Items (total)	P1	P2	P3
1	Governance	Chris Brocklesby / Kelly Goodwin	13	8	2	3
2	Software Delivery	Zdravko Mladenov	17	13	4	0
3	Security	Dean Bessell	19	17	2	0
4	Business Support	Mike Braithwaite	5	5	0	0
5	Transaction Integrity	Luke Bailey / Brian Hogg	5	3	2	0
6	Retail	Andrew Kingham	14	10	4	0
7	Legal & Regulatory Compliance	Sarah Clayton	22	8	6	8
8	CIU/Speak up	John Bartlett	55	55	0	0
9	Data	Chris Russell	23	20	3	0
10	Culture	Tim Perkins	14	12	2	0
11	Finance	Tom Lee	8	8	0	0
12	Contract Management	Liam Carroll	8	8	0	0
13	Gating & Business Readiness	Sherin Paul	14	1	1	12
14	Inquiry Thematic	Hema Kanani	67	67	0	0
15	Second Device	Brian Hogg	0	0	0	0
Total			284	235	26	23



On what basis with the Integrated Assurance Universe be prioritised?

The allocation of P1, P2 and P3 classifications will need to be confirmed by the identified by the universe areas / domain owners to ensure these are prioritised in accordance with their impact to go no go decisions/gateways.

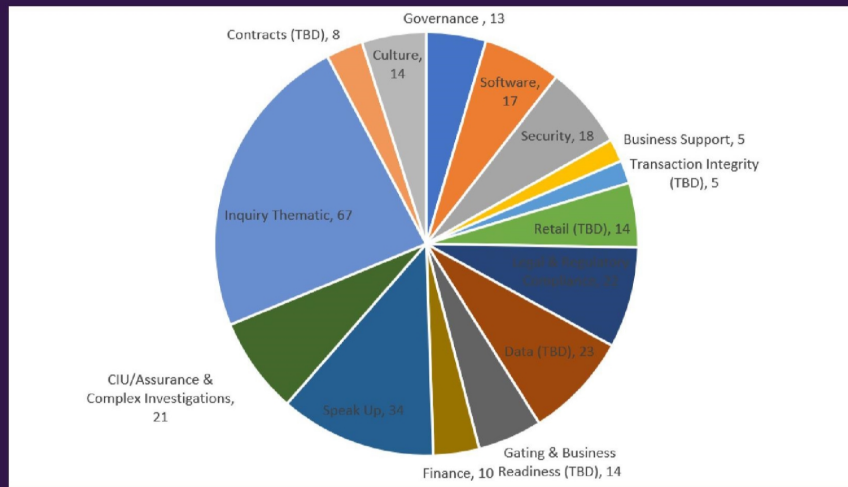
Assurance work plan and scheduling of activity will be created based on the ratings provided and future release go live dates. To ensure any assurance activity results are provided before go live decisions are taken

P1	If no assurance is undertaken, it could have a material effect on any go/no go decision
P2	If no assurance is undertaken, it will not have a material effect on go/no go decisions but may have a material effect further down the line
P3	If no assurance is undertaken, it will not likely have a material effect on the programme but could crystalize as a risk event in the future



Coverage of Risks

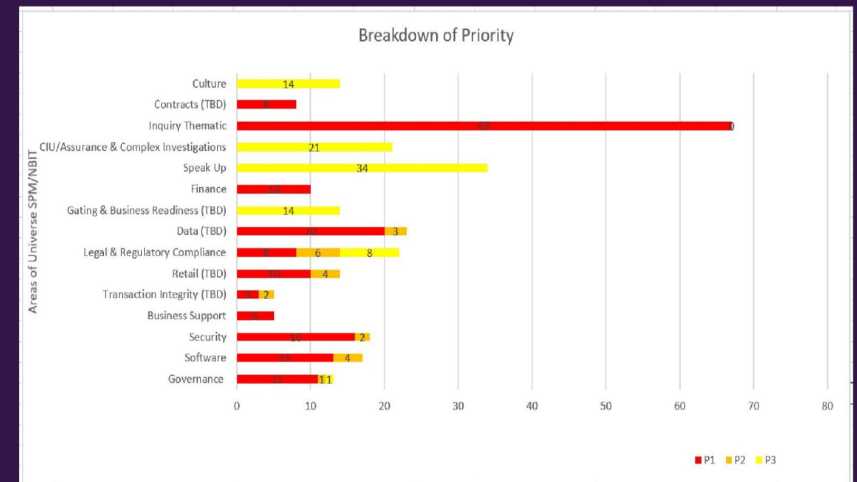
Categories broken down by number of line items and volume in the universe



Notes:

- Areas require validation for completeness / accuracy
- Ratios could change as they are validated by owners

Weighting by prioritisation across universe areas



Notes:

- Areas require validation for completeness / accuracy to ensure the priorities are agreed by owners and relevant stakeholders.

What are the main areas of risk in the Integrated Assurance Universe?



These diagrams provide an example of the look and feel of the Integrated Assurance Universe

Each of the areas will have their own

Articulation of risk

- Dependencies if any, across universe areas
- Key indicators / monitoring and
- Mapping to the relevant observations from the Inquiry

Links to Universe Framework and Strategy

- [Master copy ver0.20 Integrated assurance plan ERM 24 October 2023 .xlsx](#)
- [Integrated Assurance Strategy.docx](#)

Assurance Universe – So What									
SPM/NBIT	Business Owner	Line Items (total)	P1	P2	P3				
Governance	Chris Brockleby / Kelly Goodwin	13	13	0	0				
Software	Matt Walton	17	13	4	0				
Security	Dean Bessell	18	16	2	0				
Business Support	Mike Braithwaite	5	5	0	0				
Transaction Integrity		5	3	2	0				
Total		54	50	4	0				
Legal & Regulatory Compliance	Sarah Clayton	22	8	6	8				
Data	Chris Russell	25	20	3	0				
Total		117	88	25	8				
Other Universe Areas	Business Owner	Line Items (total)	P1	P2	P3				
Gating & Business Readiness		14	14	0	0				
Finance	Tom Lee	10	10	0	0				
CHU/Donk up	John Bartlett	35	35	0	0				
Inquiry Thematic		67	67	0	0				
Contracting		8	8	0	0				
Culture	Tim Perkins	14	12	2	0				
Total		108	102	2	0				

Risk Area (L1)	Ref	L2 Risk (root cause)	IRR	Inherent Risk (IR)	Dependencies	Monitoring	Inquiry Assurance
Software Delivery	SD2.1	Business Requirements - Capturing of Business requirements do not follow a standardised framework to ensure completeness, accuracy, and appropriateness.	P2	Without following a robust process of obtaining, reviewing and signing off business requirements from SME, stakeholders and Product Managers, there is a risk that systematically SPM would not meet the requirements of its business case i.e. not fit for purpose, inadequate control environment, inability to enforce legal and regulatory requirements, inability to overtly protect the interest of key stakeholders (PM and Customers).	TBD	TBD	TBD
	SD2.2	Non Functional requirements - Non-functional requirements are not fully complete at the time of review and are being drafted, including security and performance requirements.	P1	In the absence of complete non-functional requirements, we would be unable to ascertain how the system design language has been defined to capture accessibility and usability requirements. Technology, operational resilience and device requirements are also not fully captured. The absence of clearly defined and prioritised requirements could result in in scope creep and missing timelines.	TBD	TBD	TBD
	SD2.3	Architecture - Mismatch between IT architecture and business needs	P1	If the IT architecture is not properly aligned with the business needs, it can result in inefficiencies, decreased productivity, and inability to achieve strategic objectives.	TBD	TBD	TBD
	SD2.4	Testing - The overall testing strategy, as well as sub-strategies such as environment(s) management, tooling, non-functional and functional testing strategies, have not been formally established, approved and communicated.	P1	The absence of an overall testing strategy, which includes processed and governance around environment management, tooling, non-functional and functional testing strategies, will result in misuse and inevitable errors.	TBD	TBD	TBD
	SD2.5	Release Planning - Lack of a robust planning for the creation, management, testing and maintenance of software	P2	If releases are not planned and tested adequately, it can lead to the introduction of errors into the live environment, causing system disruptions, degradation of service quality, and potential damage to the organisation's reputation.	TBD	TBD	TBD
	SD2.6	Functional Testing - Ineffective framework for testing, assessment of defects and associated risks e.g. quality assurance	P1	If the testing process is not robust, structured and repeatable, it can lead to segregation of duties conflicts, inconsistent test results, missed defects, and inappropriate defect risk assessment and increased risk of service and/or operational failures.	TBD	TBD	TBD
	SD2.7	Code Development - Code developed not in line with POL requirements, improvements from legacy systems and industry best practice	P1	If software development processes do not adhere to established SDLC standards, it can lead to poor code quality, security vulnerabilities and lack of adoption by end users.	TBD	TBD	TBD
	SD2.8	Code Deployment - Inadequate governance and strategy on the management of all environments used within SPM e.g. deployments e.g. Development, UAT, BVT,	P1	Software development processes do not incorporate requirements for process testing to minimise system downtime, loss of data, or other service disruptions in the event a deployment needs to be reversed. This could negatively impact the business operations and reputation.	TBD	TBD	TBD
	SD2.9	Backup and Recovery - Lack of back up and recovery planning for releases into branches	P1	If a back up and recovery plan is not created and tested, in the event of an actual incident, the application could not be restored timely, resulting in reputational impact and loss of revenue for the POL.	TBD	TBD	TBD



What will our work plan look like?

The work plan will include:

- How much assurance coverage we have within SPM (i.e., self assessment completed by domain areas)
- The extent to which lines of defence will be assured incrementally etc.
- Specifically, the level of first line coverage (and if any third line coverage, if time is available)

The goal of a robust workplan is to report and track against three main questions:

- Have we done what we and the business were supposed to have done/assured?
- What was the outcome?
- What is our opinion on the control environment for that period?. Has it been effectively integrated?

Draft 2024 workplan

(contingent on POL / SPM completion and ownership of the Integrated Assurance Universe)

Review Name (work packages)	Ref #	Sub Areas from Universe	Owner	1st Line of Defence	2nd Line of Defence	3rd Line of Defence	External	Test Assurance Lead	Priority ratings	Draft Control Environment Rating	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
Assurance SPM 1 - Review Name	SD2.6	Functional Testing	Matt Walton		Yes			Anshu Mathur	P1													
	SD2.11	Defect Management	Matt Walton	Yes				Thomas Tedman	P1													
	SD2.15	Functional Testing - UX/UI/Accessibility	Matt Walton	Yes				xxxx	P1													
	SD2.17	Release Management	Matt Walton	Yes				xxxx	P1													
	SD2.14	Change Management	Matt Walton	Yes				xxxx	P1													
Assurance SPM 2 - Review Name	SD2.2	Non Functional Testing	Matt Walton	Yes				xxxx	P1													
	Sec3.2	Security Logs and Audit requirements	Dean Bessell	Yes				xxxx	P1													
	Sec3.10	Privileged Access	Dean Bessell	Yes				xxxx	P1													
	Sec3.13	Data Security	Dean Bessell	Yes				xxxx	P1													
	Sec3.3	Design & Code Reviews	Dean Bessell	Yes				xxxx	P1													
Assurance SPM 3 - Review Name	SD2.12	Source Code & Environment Management	Matt Walton	Yes				xxxx	P1													
	Sec3.15	Network Security	Dean Bessell	Yes				xxxx	P1													
	Sec3.16	Compromise Resiliency	Dean Bessell	Yes				xxxx	P1													
	SD2.3	Architecture	Matt Walton	Yes				xxxx	P1													
	SD2.8	Code Deployment	Matt Walton	Yes				xxxx	P1													
Assurance SPM 4 - Review Name	Gov1.2	Programme Structure, Roles & Responsibility	Lee Hordford	Yes				xxxx	P1													
Internal Audit: (3rd Line)	IA	SPM Quarterly / Half Yearly Audit	Johann Appel			Yes		Tim Bennett	P1													

Factors used to determine work packages:

- Risk basis (P1,2,3) – i.e., whether critical to go live and / or governance
- Utilisation of internal resources versus external SME
- Opportunities to leverage existing assurance (if possible)
- Opportunities to leverage third line external relationships

Where possible, packages will be aggregated to ensure efficiency, coverage of interdependencies and / or one time assurance. The work package may be a combination of coverage areas (i.e., this is not being done in a siloed or myopic manner).



What are the options for SPM Assurance?

Option	Description
1 <u>Pause the programme</u> while assurance catches up	Assess Assurance conducted to date which may no longer be reliable and so may need to be reperformed and / or widened for adequate coverage and completeness (i.e., the basics)
2 <u>Conduct a targeted Assurance review</u> to assess state of readiness	Leverage known assurance reports (where possible) and the Accenture review to assess what has been delivered to date, understanding whether the programme / POL can demonstrate that robust procedures have been applied, touching on key aspects of programme delivery (e.g., risk management, business requirements, end-to-end delivery life cycle)
3 <u>Perform a desk-top / black box assurance review</u> over artefacts the programmes provide for current go / no-go releases	Support a go / no-go opinion through a desk-top / black site assurance review; this is likely to be of limited value and so is the least preferred option
4 <u>Continue SPM releases</u> in absence of assurance	Continue releases without assurance, provided residual exposure is defined, assessed and monitored
5 <u>Hire external support to help complete assurance</u>	Hire external assurance capability to work with POL assurance (SPM) to provide first line assurance across the SPM programme using the SPM integrated Universe



SPM Assurance - Key Steps/ Actions

	Description	Timeline
1	<u>Complete build of the Assurance Universe</u> Ensure completeness, accuracy and risk prioritisation has been validated via SPM / Business Owners.	10 Jan 2023
2	<u>Create and agree an Integrated Assurance Plan / Work packages</u> <u>Focusing on P1 Assurance Universe line items</u> , build an Assurance work plan ie what needs to be assured as a minimum baseline, and identify resources and costs needed ie internal and or external	15 Jan 2023
3	<u>Release Alignment</u> Using step 2 above, assess what assurance can be relied on ie the baseline, and the implication to go live(s) past and planned, ie risks that have not been assured, but must be	10 Jan 2023
4	<u>Execute Prioritised Assurance Work plans</u> Execute Assurance activities per timelines agreed	10 Jan 2023

For the user - ensure the user is aware



APPENDIX



What previous audits and assurances have taken place within SPM / NBIT?

Caveat: These have not been consumed in the Integrated Assurance Universe or assessed for reliability

FY	Period	Review	LOD	Area / Delivery	Reviewer
FY21/22	May – Jun 21	SPM Programme Business Case Review	3rd Line	Business Case Review	IA/Deloitte
FY21/22	01/07/2021	SPM Programme Business Case Review	3rd Line	Business Case Review	IA/Deloitte
FY21/22	Aug – Sep 21	T&C Transaction Integrity Assurance	3rd Line	R1	Credera
FY21/22	01/10/2021	SPM MVP Pilot Deployment (D&C GO/NO/Go	3rd Line	GO/NO/GO Criteria Review	KPMG
FY21/22	Oct 21 – Jan 22	SPM Programme Set-Up and Governance Audit	3rd Line	R1	IA/Deloitte
FY21/22	Apr – May 22	SPM Set-Up and Governance (follow up from Oct 21	3rd Line	R1	IA/Deloitte
FY22/23	Apr 22 – Jun 22	Slim Counter Review	1st Line	R1 E2E Review NBIT Slim Counter	Assurance Unit NBIT
FY22/23	01/08/22	External Advisory Review to assess progress made since Sept-21 external review with new recommendations	1st Line	R1	Credera
FY22/23	Aug 22 – Oct 22	SPMP –Milestone 1 (Counter Pilot	1st Line	R1	IA/Deloitte
FY22/23	01/10/2022	Drop and Collect Review	1st Line	R1	Credera
FY22/23	01/10/2022	R1 Lessons Learnt (Internal)	1st Line	R1	Assurance Unit NBIT
FY22/23	18-20 Jan 23	Gating Review	3rd Line	Prog Status Review	BEIS
FY22/23	Mar/Apr 23	Technical review (code/standards/methodology	1st Line	R2	Credera
FY22/23	Mar 23	Gating Process – R2 Review	1st Line	R2 Slalom	
FY22/23	Mar 23	Assurance Strategy	2nd Line	E2E Assurance universe dev	Mazars
FY22/23	Jun 23	Test Assurance	1st Line	R2	EY
FY22/23	Jun 23	Credera Tech Review	1st Line	R2	Credera

Retail Assurance

RETAIL UNIVERSE DRAFT WORKPLAN

DRAFT Assurance Principles and Approach

TBC



Purpose

Purpose of today's session is to provide an overview of the Retail Assurance workplan and discuss and agree principles for the way forward.

Retail are accountable for ensuring they own and have appropriate oversight of their Retail Universe.

Group Assurance along with other assurance functions (Compliance and Internal Audit) are responsible for monitoring the control environment on an objective and or independent perspective ie the 3 LoD

Group Assurance will **TBC**:

- On a sample basis objectively validate the assurance activities of the Retail team; and
- Complete 'spot checks' on roughly 25% of the completed activities/universe

ARC Commitment

Reporting to ARC in January 2024 will comprise the approach agreed, and plan (ie number of) for commencement of assurance activity.

Retail Universe – Pragmatic risk distribution

	P1	P2	P3	Grand Total
CIJ1 - Onboarding	4	5	3	12
CIJ2 - Training	10	5	3	18
CIJ3 - Branch Assurance	3	7	1	11
CIJ4 - Shortfalls	6	5	1	12
CIJ5 - Loss Prevention	6	4	2	12
CIJ6 - TC and Disputes	4	4	2	10
CIJ7 - Suspensions	4	6	2	12
CIJ8 - Terminations	3	6	3	12
Total	40	42	17	99

Risk definitions

- **P1 – Quarterly** – If no assurance is undertaken, this could have an **immediate and significant material effect** on operational processes and impact the Postmaster detrimentally.
- **P2 – Bi-annually** – These risks are not time critical however if no assurance is undertaken, the consequence of the risk materialising may **not be immediate but could still affect operational processes and impact the Postmaster.**
- **P3 – Annually** – These risks are **not time critical and less significant**, however if no assurance is undertaken, the consequence of the risk materialising may impact on operational processes causing Postmaster detriment.

Retail Universe Draft Workplan

Size of the Retail Universe

Q4	P1			P2			P3		
	Total	Retail	GA/Comp	Total	Retail	GA/Comp	Total	Retail	GA/Comp
CIJ1 - Onboarding	4	2	2	5	0	5	3	2	1
CIJ2 - Training	10	8	2	5	4	1	3	3	0
CIJ4 - Shortfalls	6	3	3	5	0	0	1	0	0
CIJ5 - Loss Prevention	6	2	4	4	0	0	2	0	0
CIJ6 - TC and Disputes	4	0	4	4	0	0	2	0	0
CIJ3 - Branch Assurance	3	2	1	7	2	5	1	1	0
CIJ7 - Suspensions	4	2	2	6	1	5	2	0	2
CIJ8 - Terminations	3	1	2	6	2	4	3	1	2
Total lines	40	20	20	29	9	20	12	7	5

P2 & P3 activity for CIJ 4, 5 & 6 will be picked up in Q1

In Q4 there are likely to be reduced number of lines as we have matched actions from the CIJ review to the Universe risks.

For example, there are 3 x P1 risks and 1 x P2 risk in CIJ 2 (Training) but these are aligned to actions with an end date of 31/3/24. This means that these lines will not be included in the final Q4 numbers. Once the actions are marked as complete, these lines will be tested in the following quarter.

Alignment where possible – will feel clunky at first.

These figures do not include P2 & P3 activity for CIJ4, 5, & 6 which are planned for Q1

Retail to provide evidence – this could be links to sites and documentation

P1 – 20 lines (50%)

P2 – 9 lines (31%)

P3 – 7 lines (41%)

In Q4, Retail will provide evidence for 36 (**12 per month**) universe line items,

Group Assurance to complete assurance

P1 – 8 (20%)

P2 – 15 (35%)

P3 – 4 (23%)

In addition, Group Assurance will review 27% Retail assurance activity and provide assurance on 27 (**c 9 per month**) line items.

Duplications – these are lines covered by other teams

Compliance team

P1 – 3

P2 – 4

P3 – 1

A&CI/QAF

P1 – 9

P2 – 1

Group Assurance will use the outputs from other Assurance functions to provide assurance.

Next Steps

Group Assurance will:

- Share the Retail Universe and the proposed work plan with the Retail team.
- Work with the retail team to provide clarity where needed.

Retail team to provide a proposal on how to deliver the workplan.

Based on the numbers in slide 4 an example of how the lines could be spread over the quarter:

Example plan								
January			February			March		
P1	P2	P3	P1	P2	P3	P1	P2	P3
6	3	1	7	3	2	7	3	2

Retail Universe Workplan

The workplan has been created using:

- Information gathered from the Retail teams (feedback from the Universe shared)
- The universe is now aligned (continue to be so iteratively) with
 - AC&I team on the Quality Assurance activity we have removed duplications which they are focussed on
 - Other assurance activities such as Compliance and Internal Audit.

How owners were identified

Collating the information provided we have allocated responsibilities as follows:

- Yellow – information to be provided by the Retail team(s)
- Pale Green - Group Assurance led activities
- Blue – Outcome of Compliance and Internal Audit assurance
- Beige – AC&I

(As defined within the Retail work plan)

