



POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	27 July 2020
Time:	14.30 - 17.00
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	Invited Attendees:
Carla Stent (Chair)	Amanda Jones (Group Retail and Franchise Network Director, Interim): Item 2
Ken McCall (SID)	James Scutt (Head of Customer Experience): Item 2
Tom Cooper (NED, UKGI)	Maxine Cross (Head of Reward and Pensions): Item 4
Zarin Patel (NED)	Tim Perkins (Head of Security, Safety & Loss Prevention): Item 5
Regular Attendees:	Amanda Bowe (Post Office Insurance ARC Chair): Item 7
Alisdair Cameron (Group CFO)	Jeff Smyth (Interim Group CIO): Item 8
Ben Foat (Group General Counsel)	Tony Jowett (CISO): Item 8
Andrew Paynter (Audit Partner, PwC)	Joseph Moussalli (Programme Manager): Item 8
Stewart Light (Audit Director, PwC)	Rob Wilkins (Cloud Services Director): Item 8
Rosie Clifton (Audit Manager, PwC)	Tim Armit (Business Continuity Manager): Item 9
Johann Appel (Head of Internal Audit)	Sarah Gray (Group Legal Director): Item 10
Mark Baldock (Head of Risk)	Hugo Sharp (Deloitte Partner)
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: 690 753 133# Pin (if applicable): 58042	

Time		Item	Owner	Action
14.30	1.	Welcome & Conflicts of Interest	Chair	Noting
14.35	2.	Policies for Approval	Jonathan Hill	Approval
		2.1 Modern Slavery Statement	Amanda Jones/ James Scutt	Recommend for Board approval
		2.2 Business Continuity Policy		
		2.3 Anti-Bribery and Corruption Policy		
		2.4 Whistleblowing Policy		
		2.5 Financial Crime Policy		
		2.6 Anti-Money Laundering and Counter Terrorist Financing Policy		
		2.7 Document Retention Policy		
		2.8 Procurement Policy		
14.45	3.	Previous Meetings	Chair	Approval
		3.1 Minutes (19 May 2020; 16 June 2020)		
		3.2 Action List		
		3.3 Draft Risk and Compliance Committee Minutes (13 July 2020)		
14.50	4.	Pensions Assurance – RM Pensions	Maxine Cross	Noting and Approval



POST OFFICE LIMITED

15.05	5.	<u>Suspense Accounts</u>		Tim Perkins/ Ben Foat	Noting and Approval
15.20	6.	<u>GDPR Update</u>		Jonathan Hill	Noting and Approval
15.30	7.	Update from Subsidiaries: verbal update Post Office Management Services (ARC)		Amanda Bowe	Discussion & Noting
15.35	8.	<u>PCI-DSS and Cyber Security Update</u>		Jeff Smyth	Noting
		8.1	PCI-DSS	Jeff Smyth	
		8.2	Cyber Security	Tony Jowett	
		8.3	Joiners, Movers, Leavers	Tony Jowett	
15.50	9.	<u>Business Continuity Update</u>		Tim Armit	Noting
16.00	10.	<u>Law & Trends Update</u>		Sarah Gray/ Ben Foat	Noting
16.10	11.	<u>Consolidated Report from Risk, Compliance and Internal Audit</u>			
16.10		11.1	Risk Report	Mark Baldock	Noting
16.25		11.2	Compliance Report	Jonathan Hill	Noting
16.40		11.3	Internal Audit Report	Johann Appel	Noting
16.55	12.	<u>Any other business</u>		All	Noting
Next ARC Meeting: Tuesday 22 September 2020 at 09.00 to 11.30 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ					



POST OFFICE LIMITED

AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	Meeting Date:	27 th July 2020
Author:	Reena Chohan	Sponsor:	Jonathan Hill/Ben Foat

Input Sought:

Discussion:

The Committee is asked to review and approve the updated Policies and the 2020/2021 Modern Slavery Statement (which requires Board approval) and endorse the proposed actions for the business to take these forward.

Executive Summary

This paper provides a summary of changes that have been made to the policies below as part of their annual review process for the ARC to consider.

Questions addressed in this paper?

1. Which policies were updated in this annual cycle review?
2. What updates were included and why?

Which policies were updated in this annual cycle review?

1. In this review cycle the following **8** policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Owner	Governance Approval Body
Modern Slavery Statement	July 2019	20/21 Statement records the progress made against previous commitments and commitments in place to continue those this financial year	Amanda Jones	RCC & ARC
Business Continuity Policy	July 2019	Changes to the CEO statement on the cover.	Jeff Smyth	RCC & ARC
Anti-Bribery and Corruption Policy	July 2019	Minor updates made – No Regulatory Changes	Ben Foat	RCC & ARC
Whistleblowing Policy	July 2019	Minor updates made – No Regulatory Changes	Ben Foat	RCC & ARC
Financial Crime Policy	Sept 2019	Legislation amendment and further enhancements made to the policy	Ben Foat	RCC & ARC

1

[Confidentiality Classification]



Anti -Money Laundering and Counter Terrorist Financing Policy	Sept 2019	Legislation amendment and further enhancements made to the policy	Ben Foat	RCC & ARC
Document Retention Policy	March 2018	Legislation and definition update.	Jeff Smyth	RCC & ARC
Procurement Policy	March 2014	Policy has substantially been rewritten to replace the previous policy dated March 2014	Alisdair Cameron	RCC & ARC

What updates were included and why?

2. A summary that identifies the changes and updates to the policies and statements have been added below:

Modern Slavery Statement:

3. The Post Office is compliant with the requirements of the Modern Slavery Act 2015 in terms of its legal obligations. It has made progress in defining what needs to be done across the business and is beginning the longer-term task of robust implementation. Post Office has prepared a new Statement for 2020/2021 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end. There are measures in place to ensure it will be published online on or before 30th September 2020
4. The 2020/2021 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2020/2021. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Good progress in 19/20 was seen across all of our commitments and in 20/21 our focus is more on maintaining and strengthening our MS procedures.

Business Continuity Policy:

5. The only changes being made to the current policy are in the CEO statement on the cover, the remainder of the Business Continuity Policy remains accurate and what we work to. The Policy is consistent with "ISO22301", which is the Business Continuity International Standard.

Anti-Bribery Corruption Policy:

6. Please refer to the annual review paper submitted. There have been no Regulatory changes to the policy, but minor amends have been made.

Whistleblowing Policy:

7. Please refer to the annual review paper submitted There have no Regulatory changes to the policy, but minor amends have been made in relation to the Whistleblowing Contact Details.

Financial Crime Policy:

8. Following review of legislation changes, incidents and assurance enhancements during 2019/20, amendments have been made to clarify terms and language and enhance some minimum control standards:

[Confidentiality Classification]



- Amended legislation section to incorporate that the 2017 MLRs have been amended by the Money Laundering and Terrorist Financing (amendment) regulations 2019
 - Amended 'Electronic' Crime to 'Cybercrime' to reflect industry norm
 - Updated associated policy references
 - New corrective control:
 - Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate money laundering or terrorist financing risks.
 - New preventative control:
 - Product and marketing managers must ensure that any product training, promotions or communications are in line with AML & CTF policy and processes
 - Enhanced minimum control standards relating to product and service risk assessment process to reflect assessment enhancements introduced in 2019/20, including new Financial Crime Engagement Tool for initial product and service assessment.
 - Minor amends to wording and definitions following Legal referral
9. With Regards to Financial Crime Policy Assurance and how the minimum required standards stated within the policy are being met, please refer to the Assurance Appendices submitted to the ARC reading room.

Anti-Money Laundering and Counter Terrorist Financing Policy:

10. Following review of legislation changes, incidents and assurance enhancements during 2019/20, amendments have been made to clarify terms and language and enhance some minimum control standards:
- Amended legislation section to incorporate that the 2017 MLRs have been amended by the Money Laundering and Terrorist Financing (amendment) regulations 2019
 - New corrective control:
 - Product Management must implement escalation procedures for when an incident is identified, so that the Financial Crime Team are made aware and if the product is outsourced to a third party, the third party is made aware. Product Management are responsible for addressing and overseeing any control failings to mitigate money laundering or terrorist financing risks.
 - New preventative control:
 - Product and marketing managers must ensure that any product training, promotions or communications are in line with AML & CTF policy and processes
 - Enhanced minimum control standards relating to product and service risk assessment process to reflect assessment enhancements introduced in 2019/20, including new Financial Crime Engagement Tool for initial product and service assessment.
 - Minor amends to wording and definitions following Legal referral
11. With Regards to AML/CTF Policy Assurance and how the minimum required standards stated within the policy are being met, please refer to the Assurance Appendices submitted to the ARC reading room.

[Confidentiality Classification]



Document Retention Policy:

12. The last annual review of the policy took place in March 2018 therefore the policy has been updated to reflect the new standardised format for Policies, given the various Document Retention Projects that have been in process the policy now reflects the changes that have come from these projects. There have also been updates to the definition section of the policy and the policy now reflects the current legislation.

Procurement Policy:

13. The previous policy dated March 2014 was brief and general in coverage. This policy document has been substantially rewritten to encompass the themes of activity within the Procurement team and to align to the new policy template that includes sections on risks and mitigation that were not a feature of the old template.

Some elements that were in the previous policy are being incorporated into the new Purchasing Policy (PP2) which is also in the process of being substantially rewritten to cover the scope of transactional purchasing activity and change of business responsibilities that is now enabled by a new procurement system.

Assurance

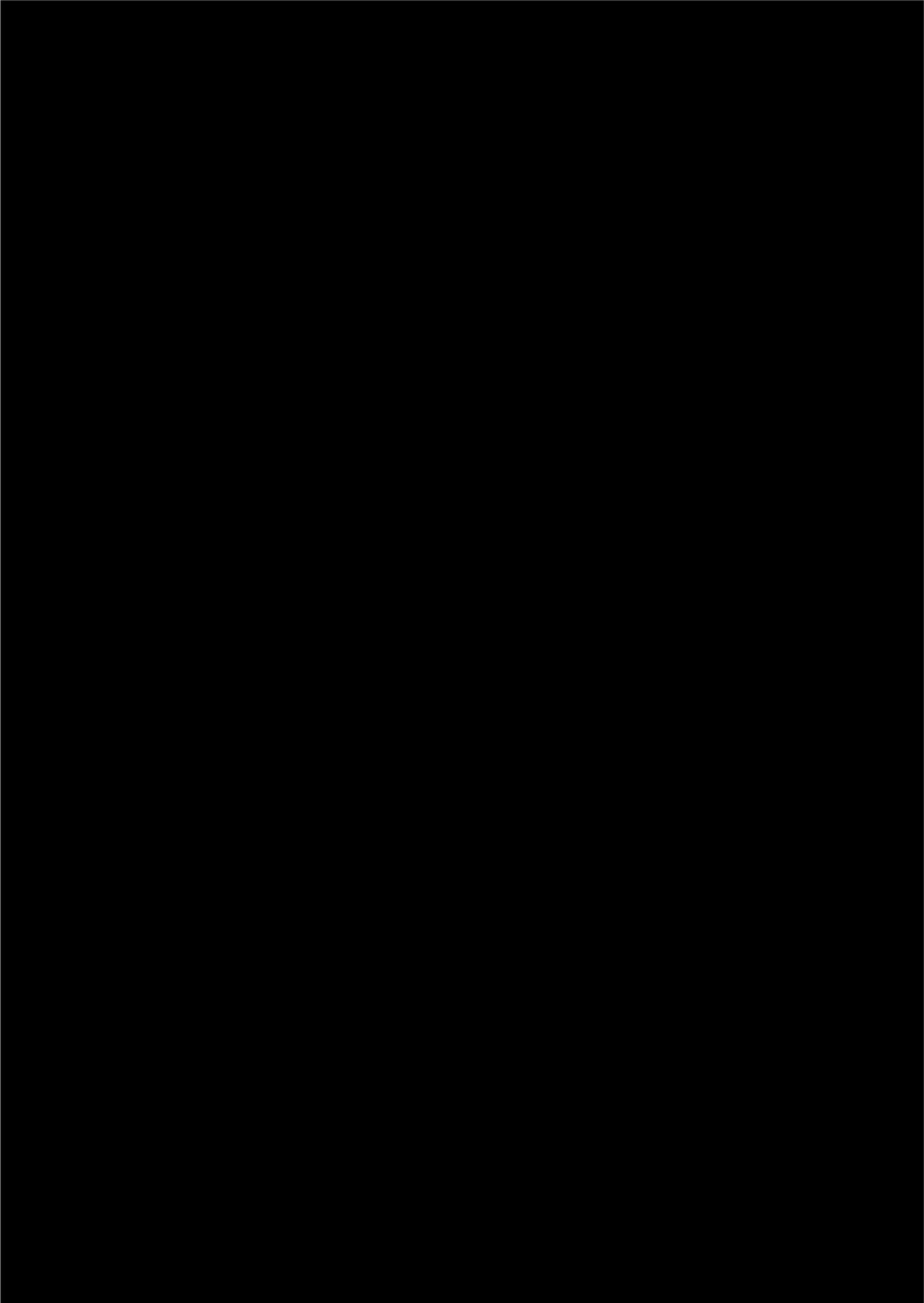
14. **After a gap in time since there had been any resource in this area, Compliance is now** working with Company Secretariat in re-establishing the key policy list for appropriate review and regular sign off as well as identifying any gaps.

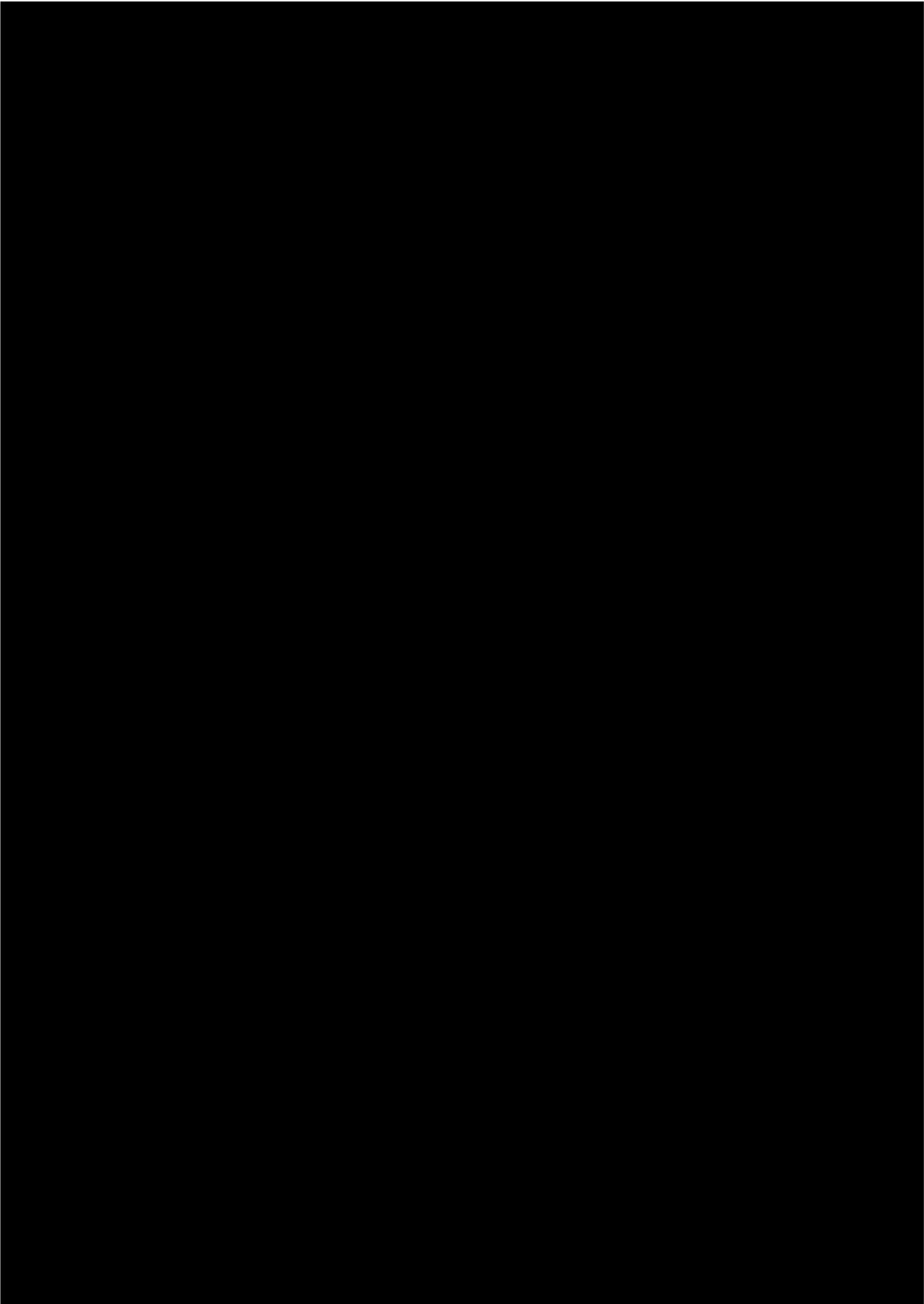
15. Compliance will also be introducing a more robust process for future policy submissions and re-review by requiring policy owners to demonstrate how the minimum control standards stated within the policy are being met. As this process moves towards BAU we would propose to sample test some of these policies on a risk basis to review the policy standard and policy compliance.

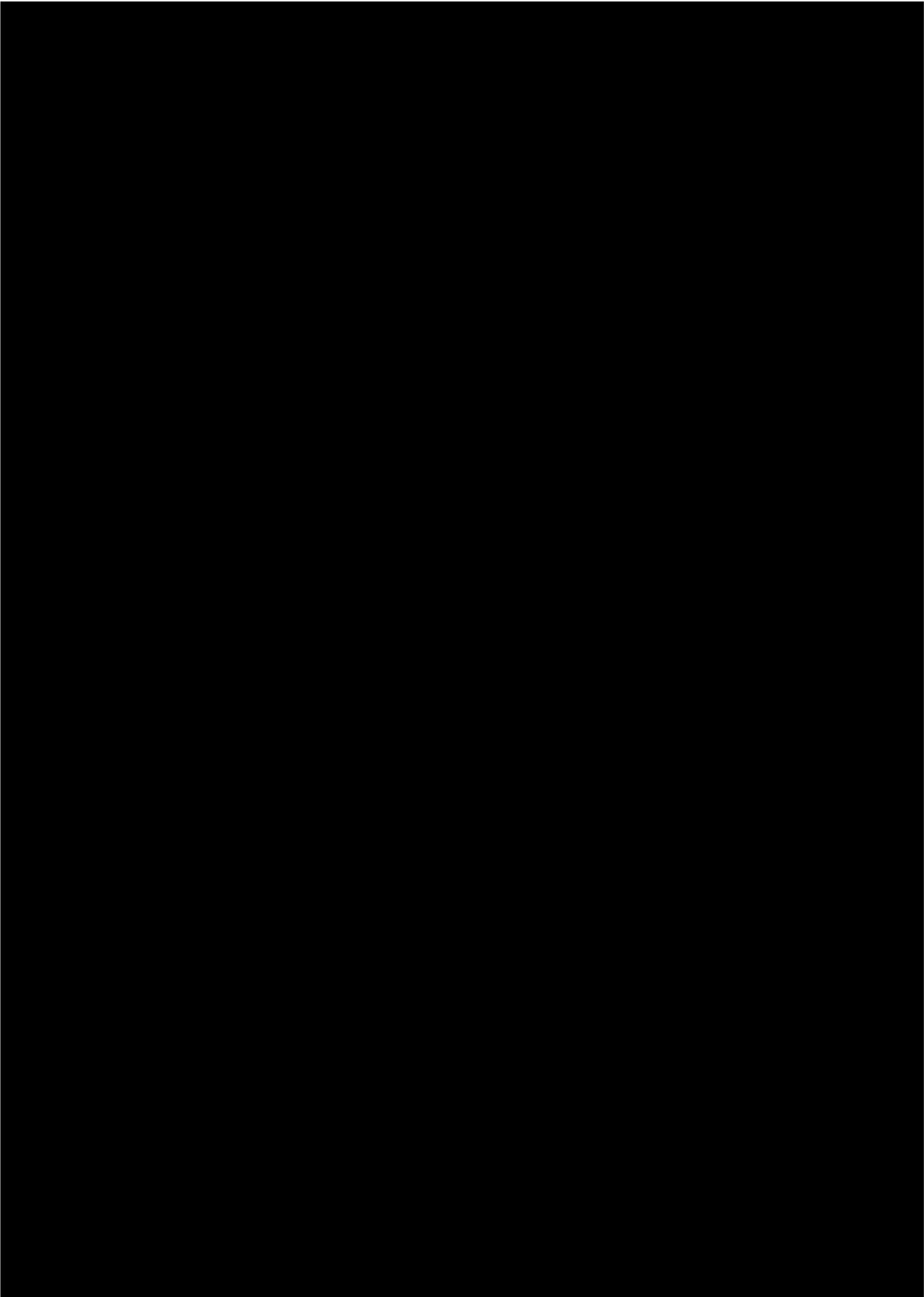
Conclusion

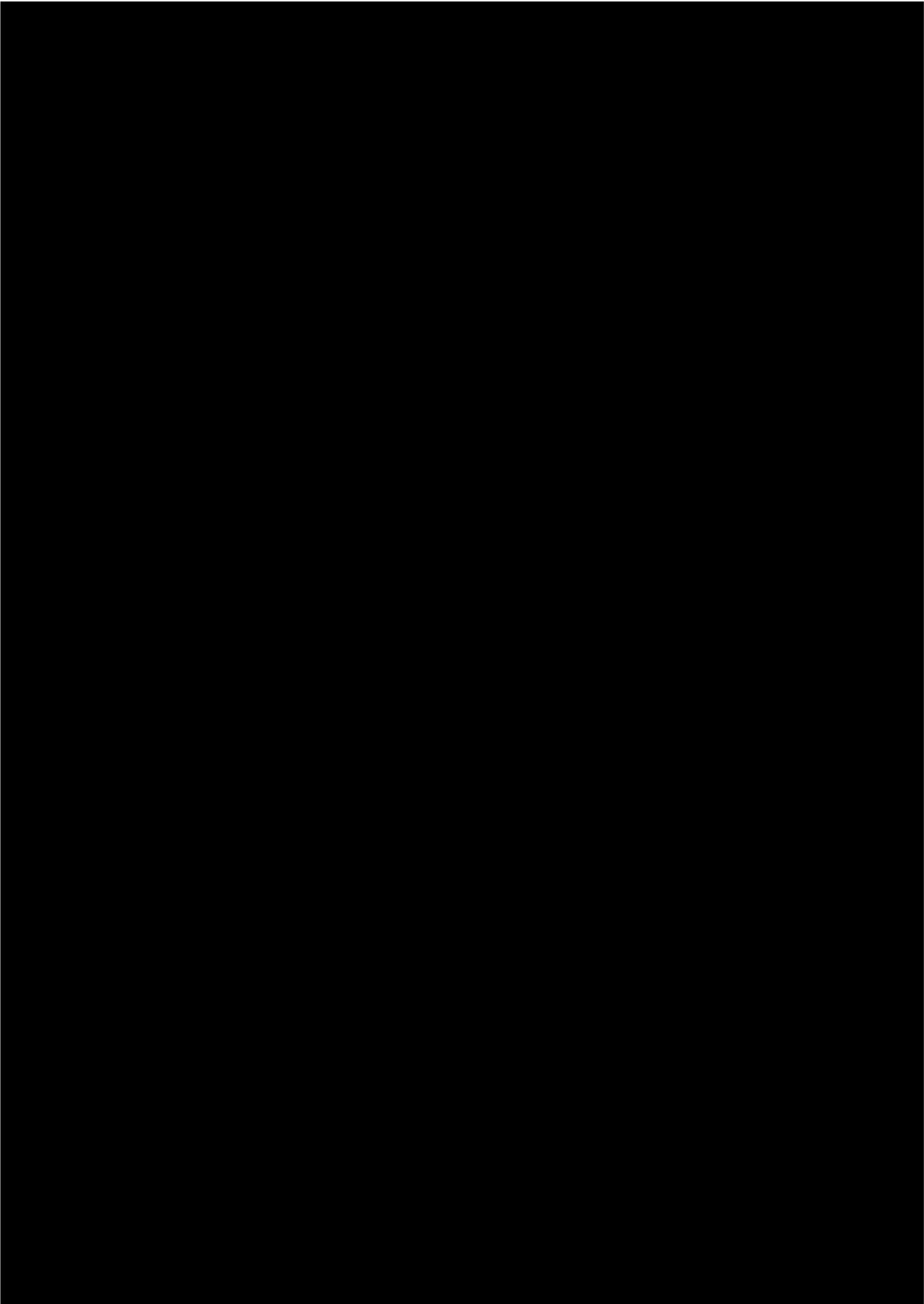
We continue to work with Policy Owners and Company Secretariat to ensure we maintain our policy governance responsibilities.

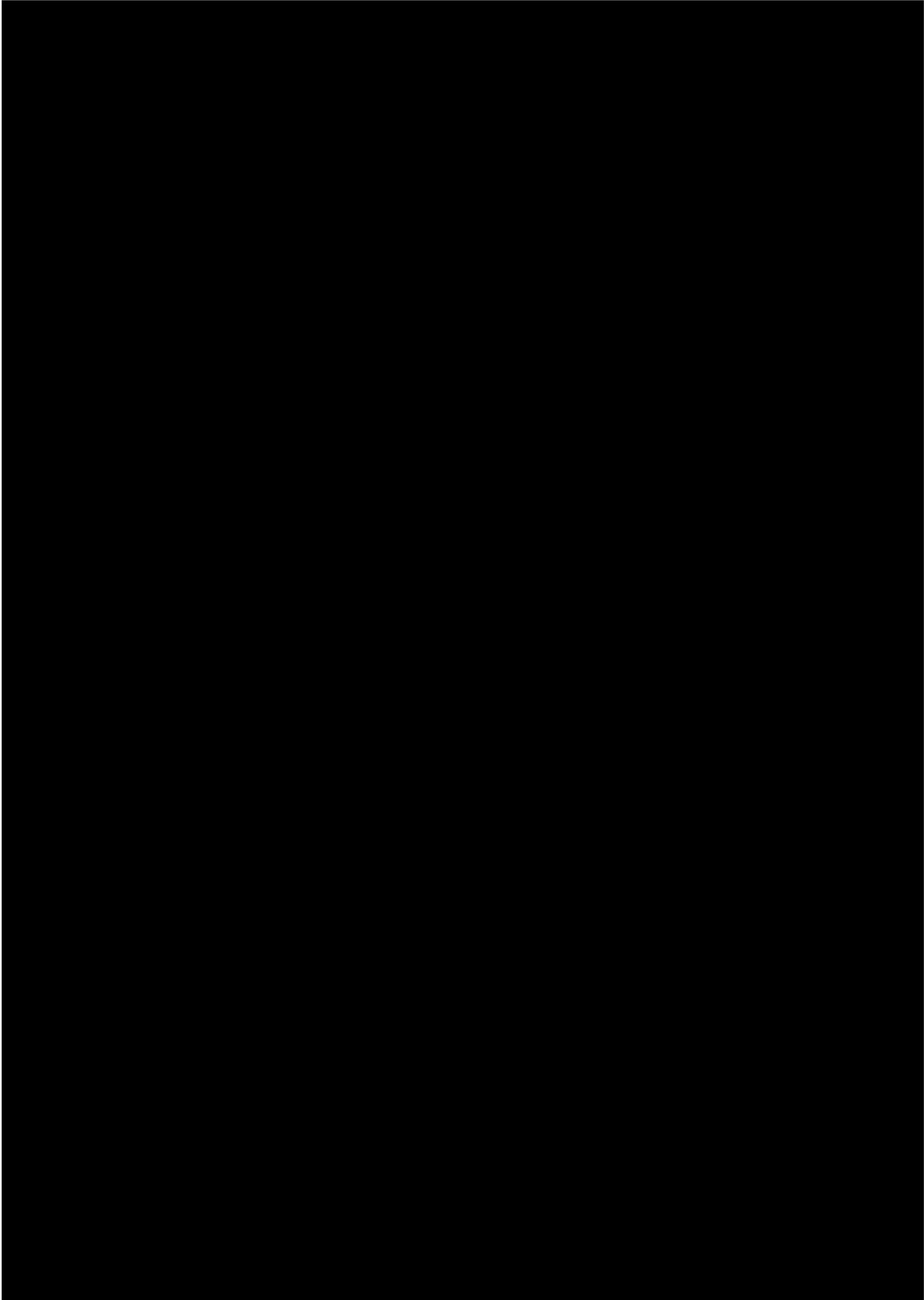
[Confidentiality Classification]

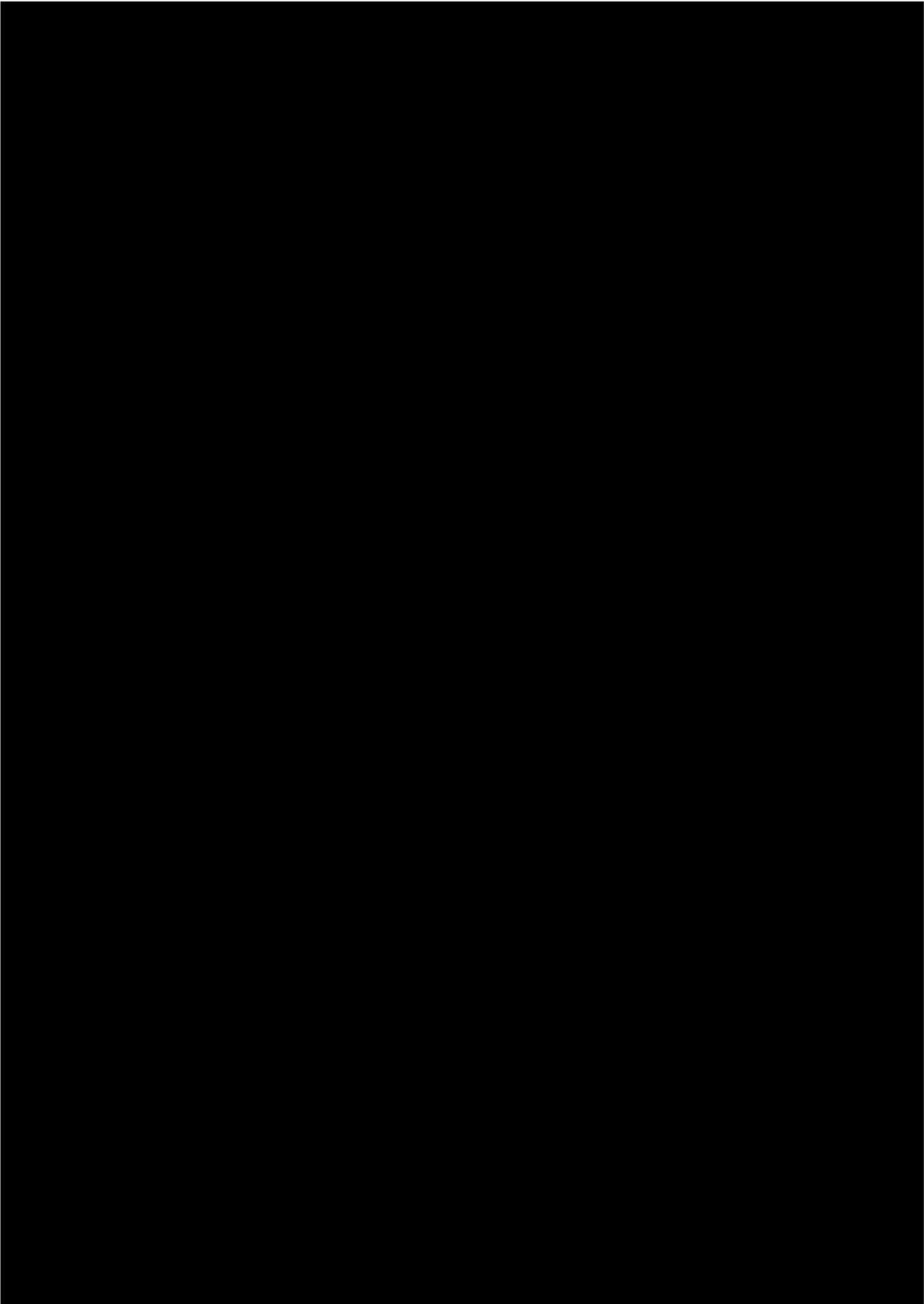


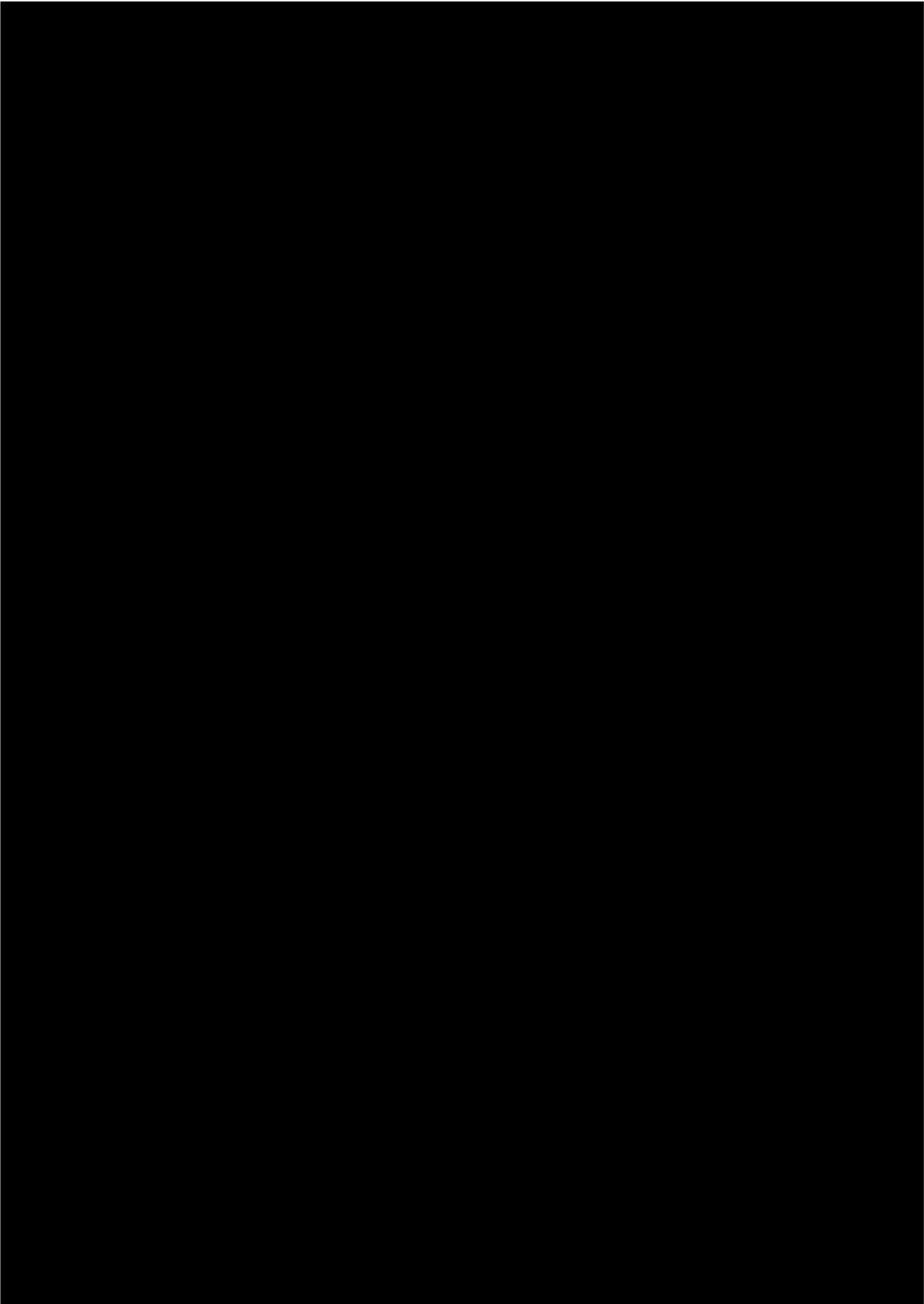


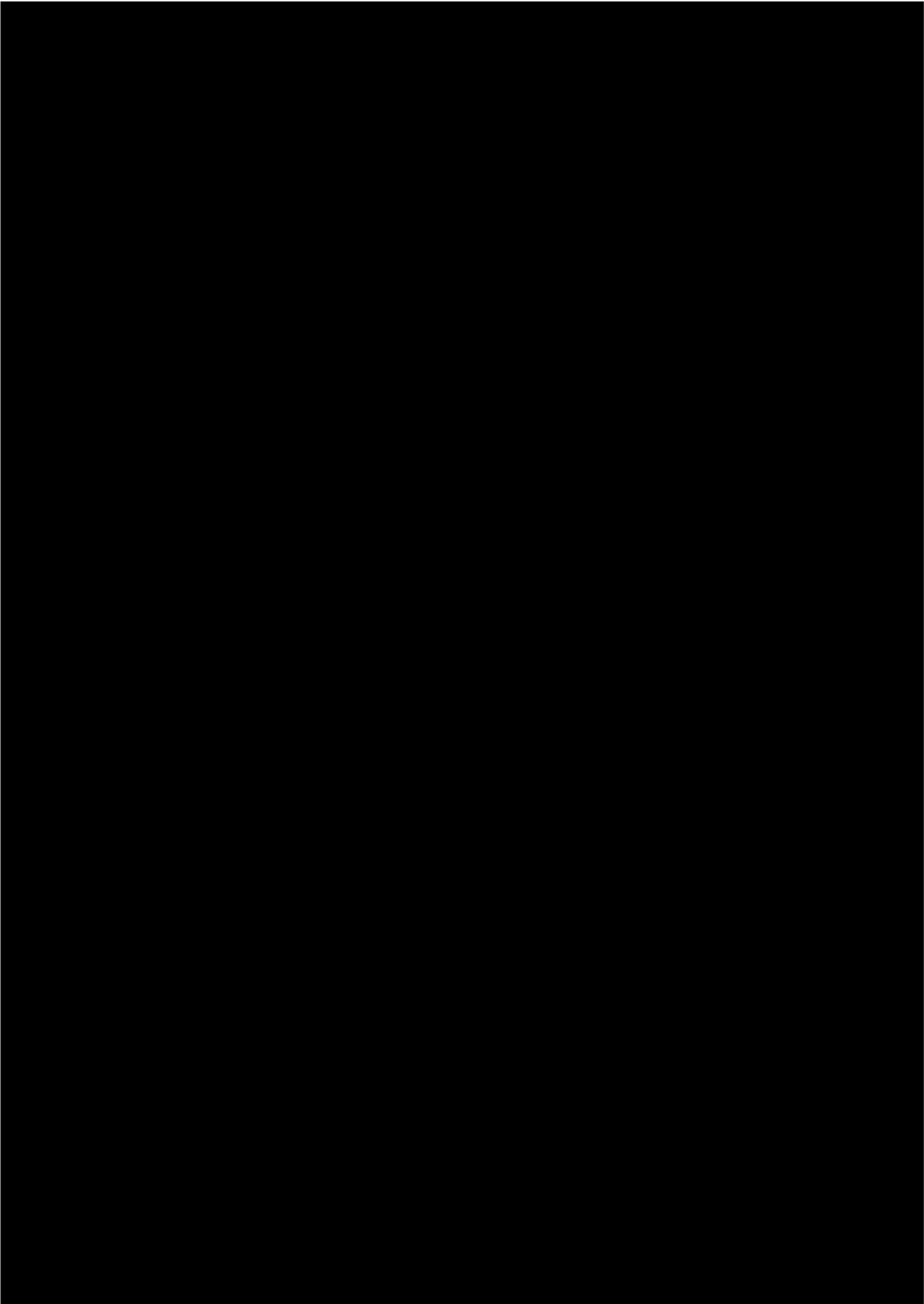


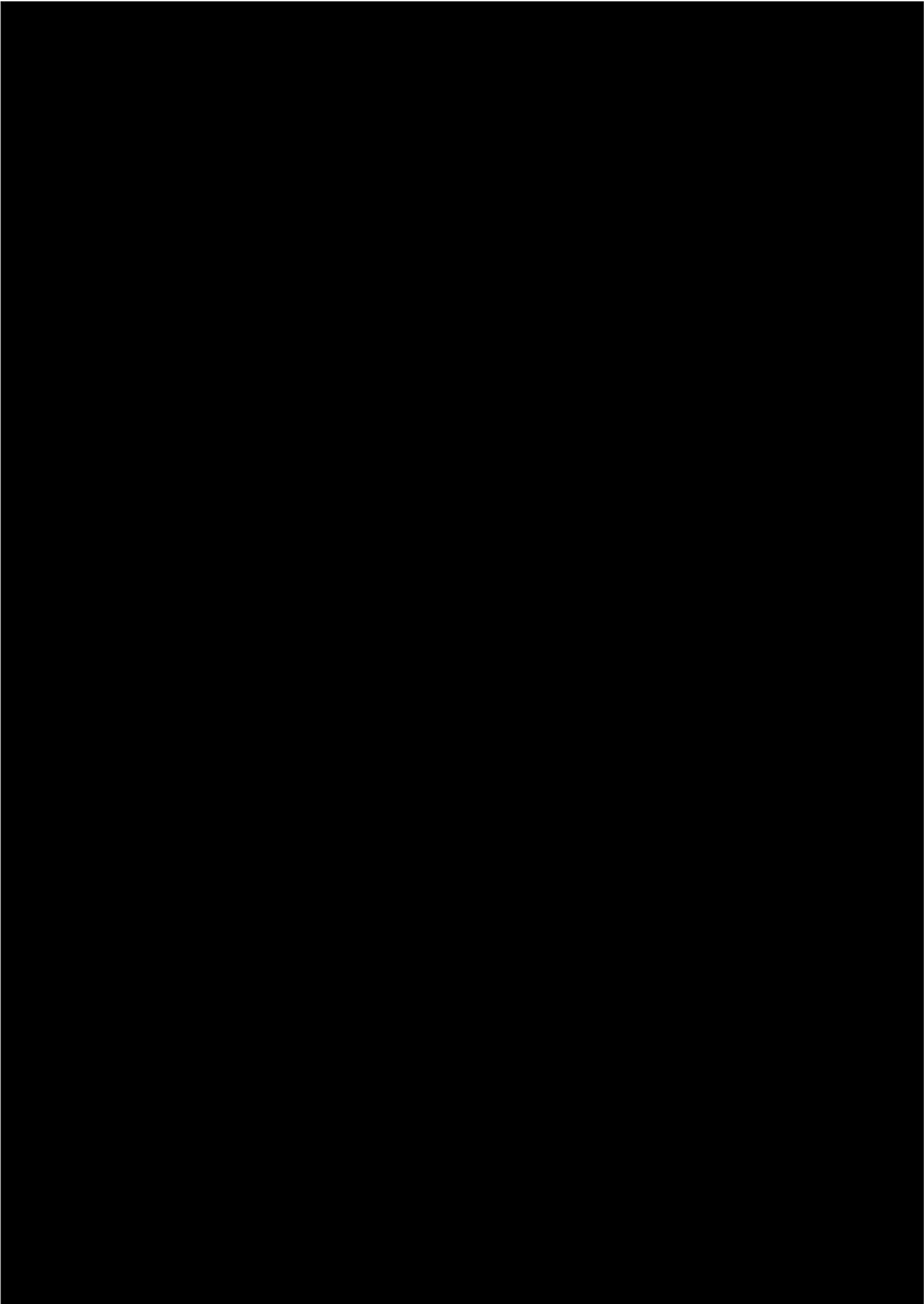


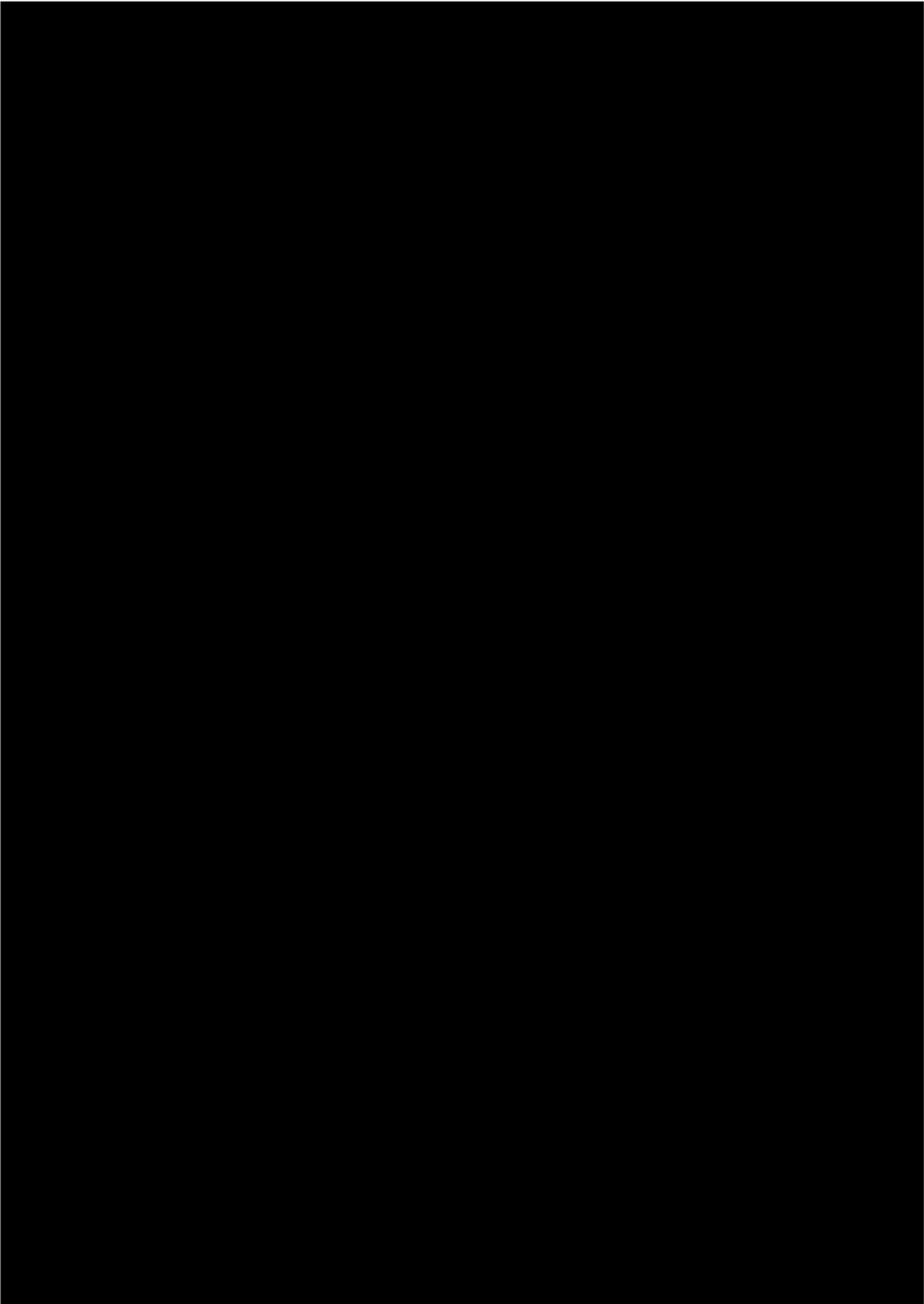














POST OFFICE LIMITED AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Annual Anti Bribery and Corruption Report	Meeting Date:	27 th July 2020
Author:	Sally Smith	Sponsor:	Ben Foat

Input Sought: Discussion

The committee is asked to review the contents of this report, approve the actions from the ABC risk assessment, updated ABC Policy, re-confirm the Corporate website statement and consider whether any further actions should be taken to improve ABC controls or gifts and hospitality reporting.

Previous Governance Oversight

The last annual ABC report and Policy amends were approved in July 2019

Executive Summary

Overall the ABC risk assessment demonstrated that control strengths have improved since the last review and did not identify any areas of material concern. The inherent risks identified are not unique to Post Office Limited and are expected as part of conducting business. The overall residual risk, although outside of risk appetite, is considered low to moderate.

The assessment has identified risk areas that require mitigation, and the full report outlines how Post Office can increase the control strength and reduce the residual risk score, and ultimately reduce its exposure to the risk of bribery and corruption. An action plan is being produced, and implementation of the recommendations, would bring the residual risk within Post Office risk appetite.

There are no material changes to the ABC policy, nor any changes to legislation since the last review.

Formal monitoring of compliance with the ABC policy minimum controls standards is in place, providing assurance that Post Office is complying with its ABC policy. Where failings are identified, these are escalated to the RCC or ARC as appropriate with recommendations to address.

The reporting and approval of gifts and hospitality has continued to improve, albeit some common errors do recur and it is likely that there is still under-reporting.



Questions addressed

1. What issues have been highlighted by the ABC risk assessment and annual review of Gifts & Hospitality?
2. What actions need to be undertaken to address any issues?
3. What changes to the Policy do we propose and why?
4. What are the implications of these changes?

Report

Summary of ABC activities 2019-20:

5. There has been no change to regulation or legislation in 2019/20, and no significant UK-based bribery and corruption cases.
6. Annual training was delivered to all employees in September 2019, and included a number of animations to re-inforce Gifts & Hospitality reporting requirements. On-going completion of training is tracked on a monthly basis, including new joiners.
7. Quarterly reporting is provided to all GE members summarising overall Post Office Gifts & Hospitality reporting and highlighting any breaches or concerns for each GE member.
8. Following a number of amendments during the year to the Gifts & Hospitality reporting tool and guidelines, there has been a marked improvement in reporting accuracy. The Gifts & Hospitality tool was completely re-built and re-launched in April 2020, with improved workflows and reporting to help drive further conformance. Some IT issues have been identified, and some modifications are currently being developed by IT to resolve. There has been minimal reporting during Covid lockdown.
9. Eight communications were issued relating to ABC and Gifts and Hospitality reporting.
10. The Corporate website ABC statement has been reviewed, but no changes are recommended (see Appendix A for current statement).
11. Activity to provide quarterly assurance of compliance with policy minimum control standards has further matured during the year, and the most up to date assessment (Q1 2020/21) can be found in Appendix D.

Annual Policy review:

12. Following the ABC risk assessment, minor amends have been made to clarify and enhance some minimum control standards:
 - Added a definition for internal bribery risks, and a minimum control standard
 - Clarified definitions relating to 'Group', 'staff' and 'employee'
 - Clarified sponsorship and charity definitions and controls
 - Added minimum control standards relating to procurement and agent on-boarding
 - Clarified some controls relating to gifts & hospitality approval

Annual Gifts & Hospitality review

15. Analysis of the 2019/20 Gifts & Hospitality Register has highlighted a slight increase in the volume of reports and the overall quality of submissions compared to 2018/19 (please



see Appendix B&C), although it is likely that some gifts and hospitality are still not being reported by recipients/offerors:

- In 2018/19 there were 47 gift reports totalling £4,918.64 and 187 hospitality reports totalling £38,703.54
- In 2019/20 there were 38 gift reports totalling £2,299.47 and 234 hospitality reports totalling £32,241.84

16. In the reporting period the following common breaches were identified:

- Further instances of employees accepting gifts of cash or cash equivalent (e.g. gift cards) from external third parties, some of which were approved by line management. In all instances the breaches were raised with line management, the cash returned and all employees in their area reminded of the policy requirements.
- Late retrospective submissions/approval after the event continue to be the most common issues. The new G&H Reporting Tool, is expected to help reduce these issues due to improved information capturing and accessibility of the tool.

17. A review of the external companies that have offered hospitality to Post Office in 2019/20 has not identified any significant issues, and the top 7 are detailed below:

External Third Party	Employee Response	Report Volume	Volume of People	Total Value
Capita Travel and Events	Accepted	3	3	£179.45
	Declined	2	2	£1,000.00
	Total	5	5	£1,179.45
MoneyGram	Accepted	12	9	£1,185.00
	Declined	0	0	£0.00
	Total	12	11	£1,185.00
Pinsent Masons	Accepted	4	13	£1,093.00
	Declined	0	0	£0.00
	Total	4	13	£1,093.00
Trethowans LLP	Accepted	1	2	£990.00
	Declined	0	0	£0.00
	Total	1	2	£990.00
Webhelp	Accepted	0	0	£0.00
	Declined	1	1	£800.00
	Total	1	1	£800.00
FRES	Accepted	6	7	£688.00
	Declined	0	0	£0.00
	Total	6	7	£688.00
Fujitsu	Accepted	3	11	£510.00
	Declined	1	1	£150.00
	Total	4	12	£660.00

Note: In 2018/19 Womble Bond Dickinson were the largest donor with 5 offers totalling £4,870, in 2019/20, POL employees received 1 offer, totalling £40.

Risk Assessment, Mitigations & Legal Implications

13. In quarter one 2020/21, an Anti-Bribery & Corruption (ABC) assessment of Post Office Limited was undertaken (a full copy of the report and recommendations is in the Reading



Room). This was the first complete assessment undertaken since the review completed in 2017/18 by Thistle Initiatives.

14. The overall control strength has seen a positive increase, and this is due to improvements in the following key areas
 - POL has new Articles of Association for all Group Companies and a framework document signed with BEIS and its shareholder representative, UKGI. The document sets out parameters within which Post Office is expected to operate, and subsequently there is more involvement from Government in decision making, reducing the risk of bribery.
 - The Procurement process, both within and outside of the scope of Procurement Contract Regulations (PCR), has improved following the implementation of a new Contract Execution Policy, the 'Source to Settle' project, and a Supplier Audit Questionnaire for due diligence on existing suppliers. In addition, since the last assessment the business has matured its approach to the approval and archiving of contracts.
 - The annual ABC training has been matured and training now includes animations to improve engagement. Greater attention has also been given to political donations and sponsorship.
 - The Financial Crime Policy Assurance Framework to measure the effectiveness of the minimum control standards in the ABC Policy on a quarterly basis has been implemented since the last review. If a substantial or sudden drop in effectiveness is identified, this is escalated to the MLRO, and where appropriate reported to the RCC and ARC. A project is also underway to identify how the existing controls can be improved.
15. An action plan is being drawn up for the recommendations from the review, which if implemented, will bring the residual risk within risk appetite:
 - In line with the Contract Management Framework the Legal team are developing, ensure signed copies of all contracts are held, these are in date and they contain the appropriate bribery clauses. Additionally, there are variations of agent contracts, which are being reviewed to ensure relevant ABC clauses are in place.
 - Implement formal assurance monitoring procedures to ensure that existing suppliers have policies and procedures which are equivalent to Post Office.
 - In line with the Compliance culture strategy under development, general adherence to group policies needs to improve, including regular certification from managers.
 - Continue to raise awareness of Gifts & Hospitality policies and procedures and monitor expense reporting against reports made on the G&H tool to identify breaches in policy.
 - The People and Policy Compliance Manager needs to work with policy owners to ensure policies are up to date and adhered to.
 - Latest versions of all policies, procedures and codes of conduct, should be up to date and readily available for all employees, with previous versions removed.
 - Publish a statement concerning charitable donations, as well as a formal approval process for employees wishing to donate to charities on behalf of Post Office.
 - Implement a process to ensure any relevant employee's affiliation to a chosen charity has been identified for a conflict of interest, with each being considered on a case by case basis.
 - Publish a statement concerning sponsorships, as well as a formal approval process for employees seeking approval from GE to accept sponsorship from a third party.



- Publish a statement concerning the award or acceptance of grants to both agent operators and employees, and ensure there are clear guidelines and controls surrounding approval.

Stakeholder Implications

16. No material changes are required to comply with the updated Policy.
17. The Financial Crime Team are working with the Head of Corporate Responsibility & Social Impact to improve processes and controls around sponsorship and charitable donations.
18. The Compliance team will work with stakeholders across the business to improve first line compliance with the ABC policy requirements as part of the overall Compliance strategy work.

Next Steps & Timelines

19. The Financial Crime Team will pursue and oversee the action plan to remediate the residual risks identified in the ABC risk assessment with relevant stakeholders during the rest of 2020/21.
20. Progress will be reported via Compliance reporting to the RCC and ARC.
21. The ABC training content is being updated and will be delivered to all employees in September 2020. On-going communication and awareness will be delivered throughout 2020/21.

Sally Smith
MLRO & Head of Financial Crime
15th July 2020



POST OFFICE LIMITED AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Annual Whistleblowing Report	Meeting Date:	27 th July 2020
Author:	Sally Smith	Sponsor:	Ben Foat

Input Sought: Discussion

The committee is asked to review the contents of this report, approve the updated Whistleblowing Policy and consider whether any further actions should be taken to improve Whistleblowing reporting and management.

Previous Governance Oversight

The last annual Whistleblowing report and Policy amends were approved in July 2019

Executive Summary

The whistleblowing process within Post Office is robust and the volume of whistleblowing reports is consistent year on year. In the last 12 months, there have been no material issues or concerns identified. Monthly MI is produced to track and monitor reports and investigations.

Further work is recommended to raise staff awareness and a continuous awareness and improvement programme is being delivered by the Financial Crime team.

Policy changes are minor and require no additional actions.



Questions addressed

1. What issues have been highlighted by the annual review of Whistleblowing reports?
2. What actions need to be undertaken to address any issues?
3. What changes to the Policy do we propose and why?
4. What are the implications of these changes?

Report

Summary of activities relating to Whistleblowing reporting 2019/20:

5. The Financial Crime team co-ordinate all whistleblowing reports and investigation on behalf of the Whistleblowing Officer, ensuring all significant or sensitive allegations are referred to the Whistleblowing Officer and that a monthly report on cases and activity is provided. A process document was created to provide guidance on how to deal with Whistleblowing reports received via all channels, including guidance for investigating managers.
6. The Financial Crime Policy Assurance Framework review which assesses if minimum control standards in policies are being met across the group was developed further during the year and the quarterly reviews have identified no deficiencies or major flaws in the application of the Whistleblowing Policy across Post Office (please refer to Appendix B for latest assurance status).
7. Our external whistleblowing reporting channels supplier, Expolink Europe Ltd, was acquired by Navex Global in June 2019. A new contract with Navex Global to provide Whistleblowing services has been completed and Post Office migrated onto their new reporting platform.
8. In 2019/20 there were 6 communications published relating to Whistleblowing to raise awareness of the reporting channels and protections, and encourage reports to be made, and some workshop sessions were held at the Employee Engagement Conference to explore ethical values and 'doing the right thing'.

Annual Policy review:

9. There have been no regulatory or legislation changes.
10. Following annual review, only minor amends have been made to clarify wording and definitions within the overview and minimum control standards sections.

Summary of Whistleblowing reports received 2019-20

11. Year on year comparison shows that there has been a slight decrease in whistleblowing reports from 43 in 2018/19 to 41 in 2019/20 (please refer to Appendix A for further details).
12. Most reports relate to individuals in the network – Postmasters and Agent Assistants as well as Post Office employees. Although there has been an increase in reports relating to colleagues in our supply chain cash centres.
13. The most popular reporting channel continues to be the Speak Up line. There has been a 59% decrease in anonymous reports being submitted, indicating that reporters have increased trust in Post Office to manage their concerns effectively.
14. The most common complaint relates to fraud, and 5 out of the 7 allegations are against Postmasters. There was also an increase in reports with allegations of Money Laundering & Bribery and Corruption.



15. There have been several reports relating to one non-customer facing location. HR continue to investigate if there are any underlying root causes or issues at this location.
16. There have been some delays in investigation caused by the Covid lockdown and inability of investigating managers to travel, but these can now be fully investigated.

Risk Assessment, Mitigations & Legal Implications

17. The new contract and the migration to the new Whistleblowing service with Navex was completed without any major problems or risks being identified. This also removed a previously identified contractual risk, for which there had been an approved risk exception note.
18. During 2019/20 there were no regulatory or legislative changes to Whistleblowing requirements, and no matters raised of material concern.

Stakeholder Implications

19. The Whistleblowing Policy makes reference to Post Office Investigations policy, specifically in relation to internal matters, however, this policy is currently out of date. The People and Policy Compliance Manager has scheduled work to get this updated for the September 2020 RCC.

Next Steps & Timelines

20. A Whistleblowing communications plan has been developed for the current year with a focus on increasing awareness around the new service and the new reporting channels.
21. Additionally a training awareness presentation or animation is planned for the second half of 2020/21.

Sally Smith
MLRO & Head of Financial Crime
15th July 2020



POST OFFICE LIMITED

3.1

MINUTES OF A MEETING OF THE AUDIT, RISK AND COMPLIANCE COMMITTEE OF POST OFFICE LIMITED HELD ON TUESDAY 19th MAY 2020 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 09.30 AM (VIA CONFERENCE CALL)¹

Present:	Invited Attendees:
Carla Stent (Chair)	Caroline Scott (Portfolio Director – Organisational Effectiveness): Item 2 (CS)
Ken McCall (SID) (KM)	Martin Hopcroft (Head of Health & Safety): Item 2 (MH)
Tom Cooper (NED, UKGI) (TC)	Rod Williams (Head of Legal – Dispute Resolution) – item 4 (RWi)
Zarin Patel (NED) (ZP)	Amanda Bowe (Post Office Insurance ARC Chair) – items 6 & 7 (AB)
Regular Attendees:	Ian Holloway (POI Director, Risk & Compliance) – item 7 (IH)
Tim Parker (Chairman, POL) (TP)	Tom Lee (Head of Finance Financial Accounting and Controls): Item 9 (TL)
Alisdair Cameron (Group CFO) (AC)	Jeff Smyth (Interim Group Chief Information Officer): Item 10.1 (JS)
Ben Foat (Group General Counsel) (BF)	Tony Jowett (Chief Information Security Officer): Item 10.2 (TJ)
Andrew Paynter (Audit Partner, PwC) (AP)	Sherrill Taggart (Interim Legal Director) – items 11 & 12 (ST)
Sarah Allen (Senior Audit Manager, PwC) (SA)	Barbara Brannon (Procurement Director) – item 13 (BB)
Johann Appel (Head of Internal Audit) (JA)	
Mark Baldock (Head of Risk) (MB)	
Jonathan Hill (Compliance Director) (JH)	
Rebecca Whibley (Assistant Company Secretary) (RW)	
Apologies:	
Nick Read (Group Chief Executive Officer) (NR)	

		Action
1.	Welcome and Conflicts of Interest	
1.1	A quorum being present, the Chair opened the meeting and noted that participation was solely by conference call given the current Government guidance on home working. However, given the requirements of the Company's Articles of Association, the location of the meeting was agreed to be the Company's Registered Office.	
1.2	The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.	

¹ Participation in the meeting was entirely via Microsoft Teams from participants' personal addresses. In such circumstances the Company's Articles of Association (Article 64) require that the location of the meeting be deemed as the chair's location. However, it was not deemed appropriate to record personal addresses on the Company record. As such, the Registered Office is recorded as the meeting location.



POST OFFICE LIMITED

3.1

2.	COVID-19 Response Update	Action
2.1	<p><i>Caroline Scott and Martin Hopcroft joined the meeting.</i></p> <p>Mark Baldock introduced the paper, which was taken as read. He noted that a COVID-19 response programme team had been set up under Caroline Scott. Over the last couple of months, the scope of the work had grown with significant implications for network coverage and financial and trading patterns. Therefore the implications were far wider than purely health and safety and the response programme reflected this. The risk work had paralleled the response programmes' phases: phase I (crisis), phase II (resilience), phase III (recover), and phase IV (Neo/Reimagine). The risk work has been two stage process: team looked at industry risks and then tested these with the business to ensure they were appropriate and all encompassing. This led to the identification of around 50 risks which have been grouped into short, medium and long term, largely mirroring the phases of the response programme. Thankfully, no areas of risk were identified by the team that were not already being picked up by the response programme team.</p>	
2.2	<p>Mark Baldock further highlighted the achievements of the response programme:</p> <ul style="list-style-type: none"> - Decisions can be taken quickly, for example, the business moved quickly and effectively to home working for all support staff including call centres and payroll. - Network coverage has been a reduction of around 10% and the branch closure figure was now stable and reducing, allowing the Network team to focus on branches closed for a number of days. - There have been patches of absence among colleagues and Postmasters, but the figure has largely stabilised. The COVID-19 related absence for colleagues stood at around 190 (which included those who were caring for a vulnerable individual or had COVID-19 symptoms themselves). - Project Neo has been set up, led by Owen Woodley. This project was to look at the longer term operational structure, target operating model and the future products and services offer. The risk team were also feeding into this work to ensure the mitigation of longer term risk. 	
2.3	<p>Caroline Scott explained that the governance around the COVID-19 response programme had ensured its efficiency. Initially, there were daily Rapid Response Team (RRT) and SteerCo meetings with all actions, decisions and risks being documented. Dashboards were used to ensure that data was the driver of decisions. A review was undertaken shortly after Easter and it was decided to move to three meetings a week for RRT and SteerCo in light of feedback from the RRT, SteerCo and GE with a focus on an integrated plan concentrating on risks. For example, much focus has been given to frontline colleague risk and extensive work has been done to identify appropriate personal protection equipment (PPE), taking into account feedback from colleagues. There has also been a focus</p>	

STRICTLY CONFIDENTIAL

2



POST OFFICE LIMITED

3.1

	<p>on the product offering and the Drop & Go product launch was accelerated in response to customers having to queue for long periods of time as branch opening hours had been curtailed and increasing social media pressure. It was also a pain point for Postmasters who felt that some customers were not posting essential items. Furthermore, the response programme team identified that opening hours information was a vital thing to get right for customers, Royal Mail (for mail collection) and Supply Chain (for cash delivery and collection). Branch Hub therefore went live as a way to communicate with branches and functionality was added to enable them to communicate their opening hours which would automatically update the branch finder tool on the customer website. Confirmation of opening hours was added as a condition of payment of top up remuneration for Postmasters in June to further drive conformance. This has driven significant adoption of the tool. 50% of Postmasters were now registered on Branch Hub and the goal was to achieve 100% by the end of the month. Such rapid adoption has been enabled by the crisis response. The Chair congratulated the team on their hard work and asked the Committee for comment.</p>	<p>Action</p>
<p>2.4</p>	<p>Tom Cooper noted that the work seemed to be all positive, and therefore queried why the reaction from the National Federation of Sub-Postmasters (NFSP) had been less than positive. Al Cameron explained that the NFSP had had an emotional reaction to the idea of linking remuneration to behaviour, however they had been talked down. He explained that conformance and, particularly cash declarations (which were another condition of remuneration payment) were a key part of our strategy and ultimately, if branches consistently did not complete cash declarations, they would be stopped from trading. It was noted that more recently, cash declarations from open branches had been slightly better than before the COVID-19 crisis. Work was also being done to consider how to support those Postmasters who cannot register on Branch Hub without creating an exception which could be used by those who can register on the system. Tom Cooper further noted that the code name of Project Neo was already known to the Minister as it had been mentioned by a contact from the Communication Workers' Union (CWU). In response, Al Cameron explained that he did not see this as an issue as it was to be expected that any business would be considering its future strategy and operating model in light of the current crisis, plus it was something that was looked at in the ordinary course of business. However, it was agreed that Al Cameron would flag this to Nick Read and Owen Woodley (Group Chief Commercial Officer).</p>	<p>AC</p>
<p>2.5</p>	<p>At the request of the chair, Martin Hopcroft explained that there was also a team looking at how colleagues could return to the workplace and risk assessments were being undertaken. Agency branches had been supplied with risk assessment proformas to enable them to undertake their own assessments where they have five or more employees. Post Office has undertaken risk assessments for Directly Managed Branches (DMBs). It was further noted that the Committee should be aware that as additional testing becomes available, there may be more positive tests and the</p>	



POST OFFICE LIMITED

3.1

	business would need to react to this. Al Cameron explained that a colleague in the Glasgow cash centre had tested positive for COVID-19 over the weekend. The response had been swift with the centre being closed for a deep clean on Monday 18 May and reopening the next day. Those who had been in contact with the colleague were traced, advised to isolate and were to be tested. In response to a question from Zarin Patel, Martin Hopcroft confirmed that the CWU had raised issues surrounding health and safety, mainly round DMB managers working on the public side of the counter. However, this was being managed with daily calls with the CWU health and safety representatives. It was recognised that this could be a further challenge as the lockdown eases.	Action
2.6	The Chair thanked Caroline Scott, Mark Baldock and Martin Hopcroft for their work on the COVID-19 response and noted that the Post Office needed to be pragmatic in its response over the next couple of months. Accordingly, the Committee NOTED the update on Post Office’s response to the COVID-19 crisis. <i>Caroline Scott and Martin Hopcroft left the meeting.</i>	
3.	Governance	
3.1	<i>Internal Audit Plan 2020/21</i> The Chair reminded the Committee that the plan had been considered at its March meeting, but that it had been requested that the plan be revised to consider the COVID-19 crisis and particularly, identify the top five priorities. Johann Appel introduced the revised Internal Audit Plan 2020/21 paper, which was taken as read. He explained that the top five priorities had now been designed and built around Post Office being able to continue to operate safely and compliantly in the current crisis. Audit proposed to examine new processes developed for the crisis response which may have relaxed controls or developed work arounds. The plan also brought forward audits that the Audit team considered to be high priority. The top five priority audits were outlined as: <ul style="list-style-type: none"> - <u>COVID-19 Programme Assurance</u>: This audit was being done in phases. A review has been done on set up and the governance of the programme, with the first interim report issued last week (this was rated green). - <u>Maintain Minimum Control Standards</u>: This audit has kicked off and phase 1 was to end this week. It was to ensure that any relaxed controls have been signed off appropriately and any new processes were being properly controlled. The audit had first considered cash controls and was now moving to financial and IT controls. - <u>Cyber Security Maturity</u>: This was to look at where the business has increased vulnerability (particularly from phishing attacks and hacking). This was to be done in short rapid phases with an interim report being issued. - <u>Health and Safety</u>: This review was in the planning stage to understand where the focus should lie. 	



POST OFFICE LIMITED

3.1

	<p>- <u>Effectiveness of the Second Line during COVID-19</u>: This audit was to ensure that where we have redeployed second line employees into first line roles, we have not been weakening second line and this was still working as expected.</p> <p>Johann Appel noted that the plan brought priority elements so there was an element of duplication in places.</p>	Action
3.1.1	<p>Zarin Patel questioned whether the Belfast Exit and PCI Compliance Programmes should be higher up on the priority list. Johann Appel agreed that they should be, but that these programmes were running slowly so had not been included in the top priorities at present. When the time was right, these would be brought forward. Zarin Patel further noted that rules had been relaxed around passwords and access and questioned what was being done to guard against branch losses to ensure there would not be future issues. Johann Appel explained that this was part of the Cyber Security Maturity review but that any changes to password rules and access had been signed off at the appropriate levels. A review of financial controls was also being undertaken. Al Cameron confirmed that his team were very active in monitoring losses and these were being tracked carefully. In response to a question from Ken McCall, it was further explained that as yet, there was no comparative data to ascertain whether branch losses were better or worse during the COVID-19 crisis. The team was focussing on the branches with the highest risk profile. At the start of the crisis, there was around £60m of cash sitting in closed branches that was not being returned to Post Office. However, since branches have started to reopen, this figure was down to £37m. There has been a reduction in burglaries and robberies. The Committee asked to see the team’s list of high-risk branches and this was to be circulated by Al Cameron.</p>	AC
3.1.2	<p>The Chair highlighted that this was clearly a plan that may require ongoing adaption. As such, the Committee NOTED the internal audit priorities during the COVID-19 crisis and APPROVED the re-prioritised internal audit plan for 2020/21.</p>	
3.2	<p><i>Internal Audit Charter Review</i></p> <p>Johann Appel introduced the revised Internal Audit Charter paper, which was taken as read. He explained that the Charter was reviewed bi-annually and as it was last approved in March 2018, it was due for review. There had been minor changes to the Charter reflecting a change in reporting lines within the Audit team. It was also confirmed that the Charter was shared with Deloitte, the internal audit co-source, who also complied with it.</p>	
3.2.2	<p>Ken McCall highlighted that a track changed version would be useful in future and that he felt that the plan should specifically call out cyber security and cash in the Role and Scope paragraph as these were particularly important at the moment. Johann Appel explained that arguably these could be read into the operational, financial and management controls as listed. He further explained that the Charter just</p>	



POST OFFICE LIMITED

3.1

		Action
	gave Internal Audit a mandate and that its remit can ultimately be as wide as necessary with the Committee’s approval. However, the Committee agreed that the elements of cash and cyber security should be specifically called out by example within the Charter. Johann Appel was asked to update this in the Charter and circulate to the Committee. In response to a question from Zarin Patel, Johann Appel also confirmed that the new Internal Audit Code of Practice had been considered when reviewing the Charter and there had been some debate as to whether to refer to this new Code or the International Standards of Internal Auditing. Ultimately, it was decided that the Charter should refer to the International Standards, although a reference to the Code and the Internal Professional Practices Framework could be added.	JA
3.2.3	<p>The Committee NOTED the Internal Audit Charter, which was updated to reflect new reporting lines and APPROVED the Internal Audit Charter for continued use for the next two years, subject to the Charter being amended to:</p> <ul style="list-style-type: none"> - specifically include cash and cyber security within its Role and Scope (paragraph 3); - move the explanation of the process to track and report audit actions from paragraph 6 to paragraph 5; and - add reference to International Professional Practices Framework and The Internal Audit Code of Practice (paragraph 11). 	JA
3.3	<p><i>Review against Terms of Reference</i></p> <p>The Chair introduced the paper which was taken as read. It was highlighted that the responsibilities under the Terms of Reference had largely been met with two outstanding items being approved in the present meeting. Accordingly, the Committee APPROVED the outcome of the review against the Terms of Reference, confirming that the responsibilities under the Terms of Reference for financial year 2019/20 have been met, with the exception of the review and approval of the Internal Audit Charter and the approval of the Internal Audit Plan, both of which were approved on 19 May 2020 and NOTED the new Terms of Reference for the Committee adopted by the Board on 8 April 2020 to reflect the new Governance Framework.</p>	
3.4	<p><i>Committee Evaluation Report</i></p> <p>The Chair introduced the Committee Evaluation Report, which was taken as read. It was noted that there were improvements on last year and the following was highlighted:</p> <ul style="list-style-type: none"> - Compliance with the regulatory landscape was a lower scoring element and a paper was now being presented (see item 12) on Law & Treads. The Committee agreed this addressed the gaps in this area. - As to the receipt of information and timeliness, it was noted that management had been good at submitting reports, even in the 	



POST OFFICE LIMITED

3.1

	<p>information. If the request was voluntary, it would be for Post Office to determine whether or not to comply on a risk-based approach.</p> <ul style="list-style-type: none"> - Any information released would be reviewed for accuracy and contain the relevant health warnings (such as if it related to HNG-X or legacy Horizon it would flag the Horizon judgement). - The material risk was information relating to HNG-A and its reliability being called into question. It was explained that where there was corroborative evidence independent of HNG-A, the risk of releasing the information was lower and release could be permitted. If the request related to court proceedings and the information was solely based on HNG-A data, the request would be referred to the Board. - Information may have to be provided and Post Office could not mitigate against the risk of any critique of HNG-A. Work was being undertaken with IT to ensure that the business can demonstrate, at any point, that HNG-A is robust and controls are in place. <p>The Committee was asked to approve the suggested approach and discuss the policy.</p>	Action
4.2	The Chair questioned whether this policy should ultimately be approved by the Board given its links to GLO. Tim Parker agreed this was a Board level decision.	
4.3	Ken McCall explained that he was uncomfortable with the wording of the policy in that in places (notably paragraph four) it seemed to suggest that Post Office was concerned that HNG-A was not reliable, which was not the case. Ben Foat explained that the policy was already being reviewed from an optics perspective and the wording was being carefully considered. It was highlighted that the Horizon judgement stated that HNG-A was robust and that the business needed to ensure that it remained robust. Zarin Patel highlighted that the Horizon judgement stated that HNG-A was "relatively robust" and the business needed to be really clear on why it believed it was robust. She further highlighted that she had concerns about the conditions on reporting crime as the crime potentially related to public money and so should be reported. The Committee agreed that the wording needed to be double and triple checked before final approval in consideration of how the policy might be perceived if it were to be made public.	BF/RWi
4.4	Accordingly, the Committee APPROVED the approach proposed in the " <i>Group Policy: Co-operation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct,</i> " subject to the comments relating to the wording of the policy as outlined in the minutes. The Committee AGREED that the final policy should be approved by the Board.	BF/RWi
4.5	<p>Post meeting note: Tom Cooper sent the following questions/comments (which would have been asked in the meeting) for Ben Foat's attention:</p> <ol style="list-style-type: none"> 1. He was under the impression that private prosecutions had ceased a few years ago, so was concerned to read about a private prosecution 	



POST OFFICE LIMITED

3.1

	<p>last year. The topic had recently been discussed in the House (particularly the House of Lords) and BEIS was reviewing what Ministers had said against the current position. Had Post Office said anything publicly on this?</p> <p>2. BEIS had committed to the Government that no future private prosecutions could be raised without BEIS being consulted first.</p> <p>3. Details of any outbound reporting, in circumstances where suspected crime would be reported to the police, should be included in the policy.</p> <p>4. There are certain situations in which Board approval is required to provide information. The policy should clarify that all such situations would come to the Board rather than management having discretion to decide whether the Board is asked to consider a particular case.</p>	Action
5.	Previous Meetings	
5.1	The minutes of the meeting of the Audit and Risk Committee held on 24 March 2020 were APPROVED and AUTHORISED for signature by the Chair.	
5.2	<p>Progress against the completion of actions as shown on the action log was NOTED and the following actions were closed:</p> <ul style="list-style-type: none"> - Action 6 (x 2) from 24 March 2020 relating to the Annual Legal Risk Report, the due diligence approach and revised contract management plan (addressed in item 11); - Action 7 from 24 March 2020 relating to the Internal Audit plan (addressed in item 3.1); - Action 10 from 24 March relating to the Contract Management Framework Update (addressed in item 11); - Action 11 from 24 March 2020 relating to Managing Procurement Relationships (a paper was provided to the Board on 8 April 2020 and this item was further addressed in item 13); - Action 13.1 from 24 March relating to PCI-DSS and the regular confirmation from the Fujitsu and Ingencio CEOs; - Action 15 relating to the Audit Update and the implementation of Archer (addressed in item 8.1); - Action 4.7 from 28 January 2020 relating to FRES review of systems; - Action 4.8 from 28 January 2020 relating to Joiners, Movers and Leavers; - Action 11.9 from 28 January 2020 relating to cookies; - Action 11.11 from 28 January 2020 relating to GDPR and Contracts Governance. - Action 5.3 from 25 November 2019 relating to Contract Management and the top 50 contracts (addressed in item 11); - Action 7.5 from 25 November 2019 relating to Commercial Partner Contingency; - Action 5.6 (x 3) from 23 September 2019 relating to PCI-DSS. <p>Action 12 from 24 March relating to Selling Regulated Products in the branch Network was to remain open as it had been agreed that an Action</p>	To do: RW Action



POST OFFICE LIMITED

3.1

	<p>Plan would be created and this was still in train. There was an update on this in item 8.2. Jonathan Hill explained that the team was working on a plan to enable Pin Pad validation for mails contents and in the meantime, training was being undertaken and Area Managers were monitoring compliance with training requirements as a priority. Ken McCall requested that Jonathan Hill speak to McKinsey as a matter of priority about this Action Plan.</p> <p>All other actions remained open.</p>	<p>JH</p>
<p>5.3</p>	<p>The draft minutes of the Risk and Compliance Committee held on 06 May 2020 were NOTED. Al Cameron highlighted four items from the minutes:</p> <ul style="list-style-type: none"> - <u>An independent review of suspense accounts as part of the GLO work</u>: This work was being undertaken by KPMG to look at suspense account processes. A report was being prepared under legal privilege, but the initial view seemed to be that the process was good and no concerns were being flagged. There was some advice on how to make the process better including a formal policy on how debits are resolved when they have passed through all resolution stages and still haven't been resolved and ensuring that the credit back log does not build up (this was to be actioned immediately). - <u>An independent review of stamps and whether any GLO implications</u>: A third party team was reviewing this to check if money was lost. This was difficult to ascertain and the work was ongoing. - <u>CBRE performance issue</u>: HSL have previously audited Post Office's health and safety procedures and have been complementary. They have now examined property compliance, which was largely outsourced to CBRE, with whom the business has had issues in the past. The audit has shown that CBRE is unreliable and the business has been relying on them. Notably, they had failed to complete a lift inspection in Chesterfield on time. The HSL view was that this was incompetency rather than fraud. Work was being undertaken to review the contract and consider options to exit them as a contractor. - <u>Work ongoing to validate historical final salaries for the defined benefit pension scheme</u>: It has been discovered that there were some errors in the calculations under the final defined benefit pension scheme. Towers Watson have agreed that there were errors. In 2014, final salaries were capped under the scheme as way of reducing cost, and the manual process determined the final salary. The process was very complicated and there could be 70 different possible allowances which had to be considered. The process was not automated and had limited oversight, however there has not been a compliant or challenge on the amount determined in the period. The assumption therefore was that we have inclined towards being generous and we have asked for this to be quantified. The time period in question was from 2014 to present. The outcomes were uncertain and there was, as yet, no 	<p>AC/BF</p> <p>AC/BF /RWi</p> <p>AC</p> <p>AC</p>



POST OFFICE LIMITED

3.1

	<p>sense of materiality, but the work was progressing with urgency. It was highlighted that there was some discretion over the final salary amount and if need be, we would correct any under payment. The business needed to consider what to do if it was found that overpayments had been made. It was explained that there is a surplus in the scheme whose purpose was to pay the liabilities, but it may be argued by the trustees that more should be paid. However, this would need to be examined once the review was complete. Audits had been done on the scheme previously, but this element was excluded from the scope because the scheme was closed and we had done a buy-in. It was further noted that the Pensions Regulator did not need to be informed provided the issue was resolved. Al Cameron would produce paper for the Committee's next meeting in July 2020.</p>	Action
6.	Update from Subsidiaries:	
6.1	<p><i>Post Office Insurance (POI) Audit, Risk & Compliance Committee (ARC)</i> <i>Amanda Bowe joined the meeting.</i></p> <p>Amanda Bowe provided a verbal update from the POI ARC. The focus in last week's meeting was on COVID-19 and the risks to POI. The business has done a fantastic job delivering the Nemesis Project (home re-engineering) and the BAU environment was operating well. Reverse stress tests have been developed to consider what COVID-19 means for performance, and then operational and customer facing risks were discussed. In addition to COVID-19 focus, there was an update from the external auditors who have a couple of questions regarding goodwill. There were also BAU updates on Internal Audit and changes were agreed to the Internal Audit plan in light of the current circumstances. The POI ARC also approved regulatory return to the Financial Conduct Authority (FCA) and received a routine update on Financial Crime. The POI was due to meet on 20 March 2020 for a deep dive on protection strategy and further discussion about potential financial mitigations. The Committee NOTED the verbal update from the POI ARC.</p>	
7.	Deep Dive: POI Risk and Compliance Update	
7.1	<p><i>Ian Holloway and Ed Dutton joined the meeting.</i></p> <p>Ian Holloway introduced the paper which was taken as read. He highlighted the following:</p> <ul style="list-style-type: none"> - The primary concern was the customer base and the need for flexibility towards customer needs during the current crisis, for example change in driving habits, travel to different and unexpected places and cancellation of travel policies without penalty. - POI stopped selling travel products in March 2020 as it was felt these could not give cover for COVID-19 risks and were largely not 	



POST OFFICE LIMITED

3.1

	<p>needed as travel was not permitted. It was hoped that these products could be sold again in June 2020.</p> <ul style="list-style-type: none"> - Cash flow was being monitored as there were no travel sales and sales of protection were lower. If sales were to continue in this trajectory, there may be a need to delay or reduce commission payment to Post Office. However, the key focuses for the business over the next few months were getting travel sales back up and running and to improve the protection strategy to maximise sales. - Aside from these risks, POI was also monitoring their third party suppliers to ensure service levels and financial performance were maintained. It was noted that so far, all had transitioned well to home working. Project Nemesis had also been completed, despite the crisis. 	Action
7.2	<p>In response to a question from Ken McCall on the write down of good-will, Ed Dutton explained that required ongoing monitoring. There was £44m of tangible goodwill assets from the original purchase of the insurance business from Bank of Ireland, but this related only to motor, home and protection. It was reviewed every year by the auditors. It is not affected by travel so there should not be an issue. Some adjustments have been made to commission rates paid to Post Office to ensure the statutory entity of POI is stable. Al Cameron further explained that all impairments were being reviewed across the organisation. There were some impairments in IT which may be written off, but otherwise there were no issues. However, post-COVID-19, we may need to consider if there would be broader business impairments. He confirmed commission rates were being reviewed already in light of the fact that there were now lower branch sales than were originally envisaged when POI was first set up. Andrew Paynter confirmed these were very live issues and that intangible assets may need to be examined again.</p>	
7.3	<p>Tom Cooper questioned POI's approach to fairly dealing with customers. Amanda Bowe explained that the POI ARC and Board had discussed whether to offer rebate on motor insurance and had been satisfied with management's proposal to reinvest any savings in renewals, rather than rebate. Ed Dutton further explained that there was an issue of practicality: POI was not an underwriter and did not, therefore, benefit from customers driving less. There have been discussions with the underwriter as to whether rebates could be offered, but there was also a budgetary intermediary between this relationship. Admiral were in a better and easier position to offer rebates, being a monoline insurer. Otherwise, only LV were also offering rebates, with others only reflecting rates to panels. The issue would continue to be monitored along with the budget to see if this could be offered in the event there was a more market wide response. It was highlighted that travel had been withdrawn from sale and these policies had been refunded. All aspects of the FCA guidance was being adhered to, including offering three months forbearance. Management was comfortable that it had done as much as it could in the circumstances.</p>	



POST OFFICE LIMITED

3.1

7.4	On People risk, Ed Dutton also outlined that morale seemed high in POI, although many would like to return to some kind of normality. A drop in productivity had not been seen but there were some of the usual concerns about colleagues with more difficult home working set ups. POI was aligned with Post Office on its People surveys and support.	Action
7.5	The Committee NOTED the report on the POI Risk and Compliance Update. <i>Amanda Bowe, Ian Holloway and Ed Dutton left the meeting.</i>	
8.	Consolidated Report from Risk, Compliance and Internal Audit	
8.1	<i>Risk Report, including update on internal controls software</i> Mark Baldock introduced the paper, which was taken as read. The COVID-19 risk response was dealt with at item 2 above. COVID-19 risks were now wrapped into non-COVID-19 risks with 15 enterprise risks identified, alongside the 54 linked intermediate risks. The key enterprise risks were outlined as: <ul style="list-style-type: none"> - <u>Commercial</u>: Post Office's commercial proposition may be unattractive because the existing products were too complex or confusing, new products were cost ineffective, unable to be scaled and unattractive to the market; - <u>Legal</u>: Post Office may be unable to comply with legislative and regulatory changes. - <u>Financial</u>: Post Office may have insufficient funding and/or uncontrolled costs in the short, medium and long-term. - <u>Technology</u>: Post Office was heavily reliant on third party suppliers and has an ageing IT infrastructure on both hardware and software components. - <u>Marketplace</u>: Post Office services and products across the various sectors may decline and/or loyalty to the Brand reduce resulting in loss in attractiveness for Postmasters, loss in revenue and reputational damage 	
8.1.2	On the implementation of Archer, all risks were expected to be on this software by the end of May 2020. This would offer greater visibility around strategic risks and the aspiration was that the next report to the Committee would be dashboard based as generated from Archer. In response to a question from Zarin Patel, it was confirmed that there were three elements of ratings for risks (inherent where there were no controls, residual risks where there was an element of judgement and a target RAG status). This would allow trends to be reported over time.	MB
8.1.3	Al Cameron explained that the Risk team had also been asked to review the Risk Appetite Statement which was last approved by the Board in January 2015. It was proving difficult to articulate statements which could be agreed and would help the decision-making process. Once this Statement was approved, this could be built into Archer and linked to the risks and trends.	MB



POST OFFICE LIMITED

3.1

	<p>was working to clarify timings and push the deadline into next year. This was a watching brief.</p> <ul style="list-style-type: none"> - <u>Use of Cookies on Internet and Apps</u>: The commercial impact of being fully compliant was understood but it had been previously agreed that we want to be “in the middle of pack.” This has been achieved and customers could choose which cookies are on/off and could change their selections. - <u>Lost HR files</u>: ICO has confirmed that it will not take any further action in respect of the loss of at least 13 Personnel boxes. This was a significant win for the business. However, work was being undertaken to ensure those who have been impacted were supported and training procedures were being refreshed. The ICO’s advisory comments would be implemented as appropriate. - <u>Belfast Data Centre Exit and move to the Cloud</u>: IT Strategy was to exit the Belfast Data Centre in 2021 and move Horizon to a cloud based solution. IT have selected AWS as the partner of choice and contract negotiations were due to commence over the next two weeks. A lot of work has been done to find the right approach in respect of data protection and the team was now working with the upstream provider and the relevant contract owners. It was confirmed that whilst this work was due to complete in September 2021, it appeared in the 2020/21 budget as work needed to start in the current financial year to ensure the completion deadline was met. - <u>Her Majesty’s Revenue and Customs (HMRC) Fit & Proper Registration Fees</u>: Post Office has requested, via contacts with Her Majesty’s Treasury (HMT) and the Department of Business, Energy and Industrial Strategy (BEIS) that HMRC either cancels the annual registration fee for 2020/21 or that it allows Post Office to delay payment until it has been able to de-register approximately 3,000 branches that were not now commercially viable for Travel Money and assessed the impact of COVID-19 on the remaining Travel Money branches. However, HMRC have today refused to allow anything other than deferring payment until 1 December 2020, with payment being based on branches registered in June. Tom Cooper noted that the Minister was about to send a letter to HMRC on this issue and questioned if it was now required. Jonathan Hill explained that the letter could not hurt as a further discussion about fees was being scheduled for three weeks’ time. - <u>Mails - Dangerous Goods Action Plan</u>: This was discussed under the actions log as outlined in item 5.2 above. 	Action
8.2.1	The Committee NOTED the Compliance update, the impact of COVID-19 on the approach to compliance, the deferment of the HMRC branch registration fees and the update on the Mails Dangerous Goods Action Plan.	
8.3	<p><i>Internal Audit Report</i></p> <p>Johann introduced the paper, which was taken as read. It was noted that last year’s audit plan was substantially completed with one audit report</p>	



POST OFFICE LIMITED

3.1

	<p>being cleared with management. This report would be circulated to the Committee once complete. The Committee raised the following points in relation to the four other audit reports presented:</p> <ul style="list-style-type: none"> - <u>Postmaster Onboarding</u>: Ken McCall questioned whether feedback had been sought from branches on the process. It was felt that this was critically important due to the sensitivities surrounding this topic. Johann explained that the audit looked at the implementation of procedures post-GLO and there had been a survey element, but that he would need to check the extent and nature of the survey. - <u>Fit & Proper</u>: Johann Appel confirmed that the Fit & Proper process remediations were due to be implemented by the end of August. The Committee questioned whether there was annual rechecks of critical individuals and noted that there should be, at least, rechecks every three years for all staff and contractors. Johann Appel confirmed that there was no process for rechecking of vetting once an individual had entered the business, but there were rechecks for Fit & Proper. All vetting was done prior to an individual joining and having access to systems. Johann Appel was asked to confirm the time periods for rechecking. 	<p>Action</p> <p>JA</p> <p>JA</p>
8.3.1	The Committee noted the progress being made with delivery of the Internal Audit programme and completion of audit actions.	
9.	Annual Report and Accounts & Audit Update	
9.1	Al Cameron introduced the paper, which was taken as read. He outlined that we had substantially, but not wholly, completed the subsequent events procedures. The PwC audit process was running smoothly, and this would flow into a June Committee meeting and a draft of the accounts would be circulated shortly. Realistically, the accounts would not be signed quickly as the funding position with Government needed to be addressed. This would improve impairment assessment and inform our going concern assessment. Work on the GLO disclosures and any potential provisions was being held off until the funding position was confirmed. Andrew Paynter confirmed there were substantial issues that needed to be picked up later but there were practical issues of leaving these key decisions until the summer	
9.2	As to the status of the audit work, Sarah Allen confirmed this was going well but there were areas that needed to progress quicker. However, on the whole, it was impressive how the teams have adapted to working and conducting the audit remotely. For example, cash counts were brought forward so they were completed before the lockdown. The IT work was now complete, and the team were a good way through their sampling and checking. Areas around revenue generation were more challenging as there were so many different revenue streams. In some instances, manual adjustments have been made outside of Horizon and these have to be added together to get to the ledger position. The Chair highlighted that the Committee needed to understand how the revenue and adjustments tie into agent remuneration and requested assurance on this matter. It	<p>PwC/ AC</p>



POST OFFICE LIMITED

3.1

	also suggested an independent review be undertaken. Al Cameron explained that the issue was the same last year and it was not particularly controversial. Andrew Paynter also confirmed it was a complexity issue for the audit and that there were only around eight complaints on agents pay per month, amounting to less than 1% of payments that give rise to complaints. It was agreed that this issue would be discussed in detail at the June meeting given the sensitivities around agent remuneration and GLO.	Action To do: RW
9.3	The Committee NOTED the PwC update on their audit of the Company for financial year 2019-20 and the status of the FY19/20 close and proposed plans for the Annual Report and Accounts ("ARA") signing.	
10.	PCI-DSS and Cyber Security Update	
10.1	<i>PCI-DSS, including broader Fujitsu relationship</i> <i>Jeff Smyth joined the meeting.</i> Jeff Smyth introduced the paper, which was taken as read. The following was highlighted: <ul style="list-style-type: none"> - Ingenico & Post Office PCI DSS Executive Call was held on 16 April 2020. - Banking API specification has been signed off; - Point to point specification has started its 12 week accreditation cycle; - COVID-19 has had no significant impact on the overall programme critical path delivery timeline at this stage. Overall, the programme was on target and delivering against its milestones. The next significant milestone was the retail accreditation from Global Payments, which would give assurance on retail side of transactions. It was hoped that the end to end banking transaction process would commence in September with accreditation in December 2020.	
10.1.1	The Chair noted that there was really good progress on this programme and Tom Cooper requested that Jeff Smyth share the presentation from the CEO to CEO session with Ingenico with the Committee.	JS
10.1.2	It was further outlined that a broader piece of work was being undertaken to look at the Fujitsu relationship across the business, particularly in relation to PCI – DSS, Telco and Freedom of Information Requests. This work was being undertaken with Lisa Harrington (Non-Executive Director) and McKinsey have done a deep dive into the Fujitsu contract. The work was looking at where the relationship was heading and where the business wants it to go (feeding into Project Neo). The work would be brought to the May and June Boards.	JS To do: RW
10.1.3	The Committee NOTED the PCI-DSS programme progress in the last reporting period.	
10.2	<i>Cyber Security</i> <i>Tony Jowett joined the meeting.</i>	



POST OFFICE LIMITED

3.1

	<p>Tony Jowett introduced the paper, which was taken as read. The following points were highlighted:</p> <ul style="list-style-type: none"> - <u>Cyber Security Maturity</u>: The business was close to maturity and Deloitte were re-testing the maturity levels at present. This was to be focussed on 20 of the 34 cyber capabilities where there has been major progress in the maturity model. An update on the actual achievement, re-baseline of the target level maturity and plans for any gap remediation would be shared with the Committee once the audit was complete. - <u>COVID-19</u>: The operating model of the back office has changed beyond recognition. Controls needed to be loosened over a short period of time to facilitate home working, and the team has also been responding to the UK National Cyber Security Centre’s (NCSC) guidance on specific threats. These related largely to phishing, malware distribution and registration of new website domains (as good copies of official websites). A phishing awareness campaign was run internally with a fake attack being sent, with follow up comms including the results of the test. - <u>Joiners/Movers/Leavers</u>: The COVID-19 crisis took some manpower away from this project but the enhanced automation process was still due to be completed by July 2020. - <u>Protecting ourselves on social media</u>: It was highlighted that it was important that all Committee members reviewed their social media presence in light of the guidance circulated to the Group Executive and Board (and contained within the paper) so as to protect themselves and the business. 	<p>Action TJ</p> <p>TJ</p>
<p>10.2.1</p>	<p>The Committee NOTED:</p> <ul style="list-style-type: none"> - the status and plans regarding our pursuit of agreed target maturity levels; - the status and plans regarding our response to the Cyber-related threats associated with COVID-19; - the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML); and - the guidance for all Risk and Compliance Committee and Committee members regarding the secure use of social media. 	
<p>11.</p>	<p>Contract Management Framework Update</p>	
<p>11.1</p>	<p><i>Sherrill Taggart joined the meeting.</i></p> <p>Ben Foat introduced the paper, which was taken as read. It was highlighted that the Contract Management Framework (CMF) had initially identified 50 material contracts, however it was now understood that there were in fact 142. The proposal was to reallocate the funding for external accredited training for contract managers to roll out the Framework to all the material contracts. For other contracts, the Framework would be applied to them over the ordinary contract life cycle. A further tranche of work to bring contracts into the Framework could be considered later when the financial position allowed. There were around 1500 contracts that would be incorporated as they come up for renewal which would be a</p>	



POST OFFICE LIMITED

3.1

	<p>period of a maximum of three years. Application of the Framework would be expediated where possible. Sherrill Taggart highlighted that the Committee should not lose sight of the new contracts coming into play which were not yet under the Framework. There were around 300 new contracts since October 2019 and there would be ongoing annual costs of around £75,000 for licences plus £35,000 admin costs as new and existing contracts were brought onto the Source to Settle system. Al Cameron explained that the process for new contracts needed to be confirmed with funding allocated so to ensure they were under the Framework. It was also confirmed that the list of 1500 may reduce as data was added to Source to Settle but that the business did have a lot of contracts due to the many different business lines.</p>	Action
11.2	<p>The Committee NOTED that:</p> <ul style="list-style-type: none"> - The implementation of the pilot of the Contract Management Framework ("CMF") was to complete, as planned, on 19 May 2020; - The projected final costs of the pilot; and - The costs, timeframes and residual risk associated with the post pilot options for the implementation of CMF across the Post Office Group as presented within the paper. <p>The Committee APPROVED the recommended approach, as outlined:</p> <ul style="list-style-type: none"> - While internal training has been provided, accredited external training would <u>not</u> be provided to identified contract managers for material contracts, accepting the risk that this may result in a baseline level of capability not being established amongst this group of individuals. - Reallocating £26k of the £80k originally included in the budget to provide external training in order to complete the upload and mapping of <u>all</u> remaining contracts identified by the Group Executive ("GE") as being material in terms of strategic and financial value by the end of June 2020 ("Material Contracts"). - The implementation of CMF across those contracts not identified as being material by the GE ("Other Contracts") be done outside of this project through the natural 'lifecycle of a contract' e.g. as they are renewed, cease or new agreements are entered into. This will take significantly longer, through BAU resource and processes, but release c£700k from the 20/21 Change Portfolio Budget. 	
12.	Law & Trends Update	
12.1	<p>Ben Foat introduced the paper which was taken as read. He explained that it ensured the proactive management of legal and regulatory risks and was an extension of the Law & Trends Forum which had been implemented by the Legal, Compliance and Governance Function. This was a cross-functional forum that identifies new and emerging regulatory and legislative requirements and considers how to operationalise the conformance within Post Office. A number of areas were highlighted in the paper:</p> <ul style="list-style-type: none"> - Streamlined Energy and Carbon Reporting Update; 	



POST OFFICE LIMITED

3.1

	<ul style="list-style-type: none"> - Morrisons Supreme Court Appeal; - IR35 'Off-Payroll' Rules Update - Employment Legislation Update; and - Business Area Update. <p>The Chair questioned why there had been an increase in the number of Suspicious Activity Reports (SARs) since June. Ben Foat advised that it was believed that this was because we had become better at spotting suspicious activity rather than there being increased activity. Nonetheless the situation was being monitored.</p>	Action
12.2	<p>The Committee NOTED the new or proposed material changes to laws and regulations this month.</p> <p><i>Sherrill Taggart left the meeting.</i></p>	
13.	Supplier Contracts out of Governance	
13.1	<p><i>Barbara Brannon joined the meeting.</i></p> <p>Barbara Brannon introduced the paper, which was taken as read. The Chair noted that the decision of the Board on 8 April 2020 was that all PCR exceptions (whatever the value) should be approved by the Board. It was agreed by the Committee that these would be reported straight to the Board from the Risk & Compliance Committee and did not need to be noted by this Committee. Barbara Brannon explained that the paper sets out (for completeness) the exceptions approved by the Board on 8 April 2020. The following pipeline contracts were highlighted:</p> <ul style="list-style-type: none"> - <u>End User Computer Services (EUC)</u>: A project has been initiated to re-procure End User Computer services for both Branch and Colleague Services. The current plan was to have a new supplier(s) in place before the end of the current contract [April 2021 with 2 years exit services] with a targeted migration by April 2021. This was due to be discussed at the GE on 22 May 2020, however it looked like the contract would be compliant. - <u>Common Digital Platform</u>: This was a tactical 2 year DOS contract which was agreed in June 2018, with a compliant six month extension option to Dec 2020 on a short term basis to allow for cloud migration and long term strategy adoption. At 31 December 2020, there would be a hard stop with no exit assistance period. Discussions were underway with the supplier to trigger the compliant six-month extension option while procurement process(es) were run. This was due to be discussed at the GE on 20 May 2020. - Contracts for Brands/Rep, Identity Services and ATM were risk items that were being reviewed given the current COVID-19 environment. 	
13.2	<p>The Chair noted that the Identity Services contract was of particular concern given additional work being generated in this area by the COVID-19 crisis. Barbara Brannon explained that the current contract with Digidentity expires in October 2020 and negotiations were on-going to</p>	



POST OFFICE LIMITED

3.1

	agree a six month extension to March 2021 in line with the expiry of the Verify contract. There was a question as to whether we proceed with the OJEU or take a different strategic approach. A six-month extension would provide additional time to consider this. This would be discussed at GE and Board in due course. Tom Cooper noted that there have been discussions in the past about whether Digidentity were the appropriate partner and Al Cameron was asked to raise this with Nick Read and Owen Woodley to ascertain exactly what was being done with respect of this work.	Action AC
13.3	In response to questions from the Committee, Barbara Brannon confirmed that there were pipeline plans for procurement over the next 3 – 5 years covering strategy, transition, technical and other risks. The procurement team hold monthly meetings with the relevant stakeholders to discuss contracts in the pipeline. Al Cameron confirmed that extensive work was being done on this and that it was just not visible to the Board. Accordingly, the Committee requested that the paper requesting approval of PCR exceptions by the Board included a 12 month overview of pipeline contracts.	BB
13.4	The Committee NOTED the contents of the Supplier Contracts out of Governance Report. <i>Barbara Brannon left the meeting.</i>	
14.	AOB	
14.1	There being no further business, the meeting was closed at 12:41.	

.....
Chair

.....
Date



POST OFFICE LIMITED

3.2

MINUTES OF A MEETING OF THE AUDIT, RISK AND COMPLIANCE COMMITTEE OF POST OFFICE LIMITED HELD ON TUESDAY 16th JUNE 2020 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 09.30 AM (VIA CONFERENCE CALL)¹

Present:	Invited Attendees:
Carla Stent (Chair)	Tom Lee (Financial Controller) (TL)
Ken McCall (SID) (KM)	
Tom Cooper (NED, UKGI) (TC)	
Zarin Patel (NED) (ZP)	
Regular Attendees:	
Tim Parker (Chairman, POL) (TP)	
Alisdair Cameron (Group CFO) (AC)	
Andrew Paynter (Audit Partner, PwC) (AP)	
Sarah Allen (Senior Audit Manager, PwC) (SA)	
Rosie Clifton (Audit Manager, PwC) (RC)	
Mark Baldock (Head of Risk) (MB)	
David Parry (Senior Assistant Company Secretary) (DP)	
Apologies:	
Nick Read (Group Chief Executive Officer) (NR)	

		Action
1.	Welcome and Conflicts of Interest	
1.1	A quorum being present, the Chair opened the meeting and noted that participation was solely by conference call given the current Government guidance on home working. However, given the requirements of the Company's Articles of Association, the location of the meeting was agreed to be the Company's Registered Office.	
1.2	The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.	
1.3	The Chair advised the purpose of the meeting was to review and status check progress made with the audit and Annual Report and Accounts (ARA) for year-end 2019/2020. She did not believe the Committee was in a position to recommend the audit and ARA for Board approval, following initial discussions held with management and the auditors.	
2.	Audit, Annual Report and Accounts for year-end 2019/2020	
2.1	Opening Comments: Appreciating that the papers were particularly complex, AC explained that delegated authority to sign off the audit and ARA would not be sought at	

¹ Participation in the meeting was entirely via Microsoft Teams from participants' personal addresses. In such circumstances the Company's Articles of Association (Article 64) require that the location of the meeting be deemed as the chair's location. However, it was not deemed appropriate to record personal addresses on the Company record. As such, the Registered Office is recorded as the meeting location.



POST OFFICE LIMITED

3.2

	<p>this stage, as the accounts could not be considered a going concern without agreed government funding. Once discussions around renewal/replacement of this facility had progressed to an appropriate level, detailed going concern analysis would be performed, including an assessment and sensitivity analysis around cash flow forecasts and trading in light of market conditions and expectations at the time.</p>	
2.2	<p>A preliminary view of the need for impairments had been taken, but no major changes were being signalled, whilst recognising that the work had to be completed in line with agreed forecasts and funding.</p> <p>As it was likely the audit and ARA would be signed later in the year, the following would have to be updated:</p> <ul style="list-style-type: none"> • The disclosures and provisions regarding GLO and Starling; and • POL's view of any subsequent events and changes in judgements, with particular regard to pension final salaries and the historical management of stamps. 	
2.3	<p>Given the tough trading year, AC believed the draft trading profit (TP) of £86m (cf £60m in 2019) was an exceptional achievement that should not be forgotten/underestimated. This was principally driven by staff and non-staff cost savings of £52m, partially offset by increased postmaster costs and a reduction in trading income.</p> <p>For bonus purposes and Remuneration Committee discussions, the budgeted TP had been increased from £74m to £88m to reflect the impact of IFRS accounting changes and capitalised GLO costs. The budget is due to be discussed ahead of Remuneration Committee and a paper presented regarding actual vs budget.</p>	
2.4	<p>Audit:</p> <p>AP presented the audit findings to the Committee.</p> <p>He noted the audit was in its seventh week of virtual field work, with credit due to both parties for their conduct and collaborative efforts in light of current 'remote working' circumstances. (Particular thanks to TL and Christine Kirby, Financial Controls Manager.)</p> <p>He advised that subject to final review the audit is substantially completed, with the exception of work around going concern, fixed asset impairments and GLO litigation. A number of procedures and conclusions remained outstanding, but no significant issues are expected and a further Committee meeting would be scheduled once the funding position and GLO outcomes are known.</p> <p>The following areas/risks were discussed in more detail.</p>	
2.5	<p>Management override of controls</p> <p>SA reported that detailed testing of key year end reconciliations had been completed and that the testing over journal posting remained outstanding.</p>	



POST OFFICE LIMITED

3.2

	<p>The team had found the complexity and volume of data challenging to manipulate, but to date, from testing up to end of P7, had identified no significant issues.</p> <p>Discussion over manual revenue postings occurred. AC recognised this was a complex area and that the fundamental processes remained in line with previous years. However he believed the internal financial controls were suitable. AP advised that their work was complete over this area and they were comfortable with the processes and postings from the sampling performed.</p>	
2.6	<p>Going concern</p> <p>AP advised that going concern was considered a significant risk (current funding with BEIS is due to expire on 31 March 2021) and that audit work in this area was in the early stages. Once funding had been agreed in principle, forecasting would be important for future profitability.</p>	
2.7	<p>Impairment of Fixed Assets</p> <p>AP noted that in response to the Covid19 pandemic, headroom was available following two waivers since year-end (one relating to the security headroom requirement on the BEIS facility, and the second relating to the 'security cushion' on the inter-creditor agreement with both BEIS and Santander until the end of June 2020) but questioned management's EBITDA forecast of £148m in 2024.</p> <p>AC advised these comments were helpful and consistent with government conversations, and that a list of tangible assets would be circulated to the Committee following a question received from TC for a breakdown.</p> <p>A second impairment test would be completed post year-end in the light of revised forecasts following Covid19, to include a review of software (considered high at £200m by ZP), technology and POI goodwill of £45m.</p>	<p>Action: AC</p>
2.8	<p>Telecoms</p> <p>The accuracy of Telecoms billing was considered a significant risk by AP, with two elements affecting their accuracy:</p> <ol style="list-style-type: none"> 1. The correct pricing rates being applied to a particular transaction; and 2. Data usage being accurate and correct. <p>The service is provided by a third party who produce a monthly detailed debtor listing (FIN2) report. Historically there has been a reconciling difference of c£500k to POL's general ledger which had increased this year to c£1m. This was being reviewed by management, however a provision was made for the variance in FY19/20.</p> <p>AC recognised this was a complex area, noting a number of issues with the third party provider, but was satisfied that no significant issues would be raised post investigation.</p>	
2.9	<p>VAT</p>	

STRICTLY CONFIDENTIAL

3



POST OFFICE LIMITED

3.2

	<p>AP noted that POL's diverse organisational structure and revenue streams contributed to a number of VAT arrangements. To date, the samples tested were consistent with FY19 audit and no significant issues had been raised.</p>	
2.10	<p>Pensions</p> <p>AP noted the two POL pension schemes (Royal Mail Pension Plan and Royal Mail Senior Executive Pension Plan, RMSEPP) currently showed a surplus position in aggregate of £0.7m. However, without access to the pensions and due to the complex nature of pension scheme accounting (in relation to defined benefit schemes), there is a risk that the pension liability is incorrectly valued at year-end resulting in material liability being understated. He recommended that this position be reviewed by the Board.</p> <p>In addition, POL had historically recognised 7% of the RMSEPP assets and liabilities with the remainder met by Royal Mail, however no concrete evidence could be provided of this position.</p> <p>AC noted the historical behaviour of Royal Mail had accepted the 93/7% split, recognising the potential difficulties this could have with current/future negotiations.</p> <p>It was AGREED that pension numbers would be reviewed, and that TC would review any internal documents he may have access to.</p> <p>KM agreed that the 93/7% split would be used by the Remuneration Committee.</p>	<p>Action: AC/TC</p>
2.11	<p>Capitalisation of Intangible Assets</p> <p>SA advised the audit had been completed and capitalisation had been applied consistently in line with the accounting framework. A number of projects that had gone live had not been transferred to fixed assets at year end, understating amortisation by £1.3m.</p> <p>AC advised he was comfortable with the overall asset position and would circulate a list of the £64m software capitalised this year.</p>	<p>Action: AC</p>
2.12	<p>IFRS16</p> <p>SA reported this was a technically complex accounting area adopted by POL for the first time. As part of this the historical onerous lease provision has been reassigned on the balance sheet to net off with the leased asset cost. This is in line with the standards.</p> <p>The audit had been completed and apart from identifying one judgemental sum of £0.63m related to a discount rate lease liability, no other issues had been identified.</p> <p>Loss making sites would continue to be monitored with a separate provision retained.</p>	

STRICTLY CONFIDENTIAL

4



POST OFFICE LIMITED

3.2

2.13	<p>GLO</p> <p>AP advised that audit work was on-going, but due to the number of uncertainties in terms of settlement, particularly surrounding the value and disclosures around the Historical Claims Process and Criminal Cases Review Commission, this should be considered a significant risk and reviewed closer to signing the ARA.</p> <p>The team would continue to work with management and Herbert Smith Freehills LLP (HSF) who were reviewing claims not previously included as part of GLO, which commenced in May 2020 for an agreed three month period.</p> <p>The Committee noted that based on discussions with HSF, there is an expectation that sufficient information should be available shortly after the three month claims window from which to make a materially reliable estimate of the settlement costs that will be incurred.</p>	
2.14	<p>Trading Profit</p> <p>SA reported the audit was mostly complete with the exception of a few areas. However no significant issues had been identified/were expected. Materiality was £9.5m.</p>	
2.15	<p>Exceptional Items</p> <p>SA noted that exceptional items were listed under "trading" with the majority of the £70m costs relating to GLO (£57m). A charge of £52m had been recognised in the Income Statement in relation to GLO.</p> <p>A £5m expense in relation to Postal Museum had now been correctly listed as an exceptional item following talks with management, initially listed as an investment.</p> <p>ZP questioned why Postal Museum costs had been exceptionalised. AC explained there had been a change to accounting policy and the value and type of expense met the exceptional requirements as per the accounting policy.</p> <p>Agents remuneration: this had increased this year to £384m (FY365m FY19), following the closure of CPO branches and the agreed new Banking Framework (from 1 January 2020) taking effect from 1 October 2019. Manual adjustments completed via Horizon totalled £22.3m with £14.7m related to Bureau de Change adjustments (Horizon nets off the purchase and sale of forex, agents are paid gross). Invoices had been reviewed and no significant issues had been identified.</p> <p>Cash: 23 cash centres had been visited to review cash counts and understand the processes and volumes of cash transacted. No significant issues had been identified.</p> <p>FRESH: clearance meetings had been held with KPMG (auditors to FRESH). KPMG had identified two adjustments above the reporting</p>	

STRICTLY CONFIDENTIAL

5



POST OFFICE LIMITED

3.2

	<p>threshold, with one affecting POL's financial statements. This error was due to the discount rate used in the goodwill impairment assessment being too low. A more appropriate rate would have resulted in an additional £1.8 million of goodwill impairment. At the 50% level, this equates to a £0.9 million reduction in POL's £28 million share of post-tax profit from joint ventures in the income statement. This was not being booked at FRESH and therefore was not booked at POL.</p>	
2.16	<p>Capitalisation for Digital Identity Costs</p> <p>AP confirmed that PwC were satisfied that £3.8m costs can be capitalised as future revenue now looks more certain (over and above the Verify income which may be less sustainable) and in excess of the cost base. In addition, the amounts will be amortised over a short period of time.</p>	
3.	<p>Annual Report and Accounts year-end 2019/2020</p>	
3.1	<p>Accountable person: TL presented the accountable person paper. The Committee noted that Nick Read (NR) is POL's accountable person responsible for the governance and usage of public funds in line with the principles of Her Majesty's Treasury's ("HMT's") Managing Public Money ("MPM"). This paper provided the assurance that NR had met these responsibilities during FY19/20.</p> <p>AC advised that a conversation had been held with NR who recognised and agreed with his responsibilities as Accountable Person.</p> <p>The Committee requested this be updated to reflect the changes required from the GLO settlement, provide clarity that the internal IT control systems were robust and to carefully consider the position mentioned regarding Horizon.</p> <p>An updated paper would be presented when the Audit and ARA was ready for sign-off.</p>	
3.2	<p>The Chair thanked the teams (POL and Audit) for the work completed to date but recognised that the Committee was not in a position to recommend the Board sign-off.</p>	
3.3	<p>Next Steps: the following next steps were noted.</p> <ul style="list-style-type: none"> • Agree with Internal Audit the scope for a "Review of the controls around manual postings to revenue" • Provide a summary of intangible assets and amortisation rates to the Committee. • Write/communicate with Royal Mail regarding the 7% pension liability, once shareholder records/documentation had been reviewed. • Circulate the sums to support the DigiIdentity database capitalisation i.e. show it has economic value • Refresh the Accountable Person paper prior to signing ARA, to include an update on GLO and its impact(s), and provide any further details on any subsequent reports to the Committee to provide assurance on key governance items. 	

STRICTLY CONFIDENTIAL

6



POST OFFICE LIMITED

3.2

	<ul style="list-style-type: none">• Prior to signing, complete the following and bring back to the Committee for review:<ul style="list-style-type: none">○ Going concern assessment (funding driven);○ GLO summary, with disclosures and provisions;○ Impairment review;○ Details of any other Post Balance Sheet Events updates.	
4.	AOB	
4.1	There being no further business, the meeting was closed at 10:55am.	

.....
Chair

.....
Date

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
16 June 2020					
2.7	Impairment of Fixed Assets: list to be circulated to committee.	AC	July	A list has been circulated.	Recommend for closure
2.10	Pensions: It was AGREED that pension numbers would be reviewed, and that TC would review any internal documents he may have access to. KM agreed that the 93/7% split would be used by the Remuneration Committee.	AC/TC	July	Tom Cooper 13/07/2020: the team has been unable to locate any evidence of this. The split will be used by the Remuneration Committee.	Recommend for closure
2.11	Capitalisation of Intangible Assets: AC to circulate a list of the £64m software capitalised this year	AC/TC	July	A list has been circulated.	Recommend for closure
19 May 2020					
2.4	Covid Response: Al Cameron would flag this* to Nick Read and Owen Woodley (Group Chief Commercial Officer). *‘This’ is the fact that the Minister is already aware of Project Neo.	AC	ASAP	Completed: Nick Read and Owen Woodley have been informed.	Recommend for Closure
3.4 Governance – Internal Audit Plan 2020/2021	The Committee asked to see the team’s list of high-risk branches and this was to be circulated by Al Cameron.	AC	July	The Branch Analysis and Audit teams continue to monitor branches with high cash risks during the Covid-19 pandemic on a weekly basis. High cash risk is determined on the value of cash held in the branch, the robbery and burglary risk rating, the completion of branch accounting (cash declarations and trading period rollovers) and the trading status of the branch (open or closed).	Recommend for closure

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

			<p>There are currently 32 high risk branches. This has fallen from 46 branches three weeks ago. In order to reduce the number of high risk branches, the Branch Analysis and Audit team follow conduct a series of escalating interventions. They are as follows:</p> <ol style="list-style-type: none"> 1. The Branch Analysis and Audit team make a telephone call to the branch to ask that the branch does one or multiple of the following within the next week: <ol style="list-style-type: none"> a. Complete a cash declaration b. Roll the branch into the correct trading period c. Accept a transaction correction d. Return excess cash 2. If the branch does not complete the agreed action(s), the Branch Analysis and Audit team complete a further telephone call offering an Area Manager/Audit Advisor visit to help with the action required. 3. If the branch are unable to resolve the issue themselves or with the support of an Area Manager/Audit Advisor, then dependent on circumstances, the provision of cash and stock will be suspended and/or the SmartIDs for the branch’s users will be suspended. <p>There is currently 1 branch that has had its cash for its ATM suspended as a result of this process (Culverstone). No branches have yet had SmartIDs suspended for their users.</p> <p>The following are the highest risk branches in the network (as at 8th June 2020):</p> <ul style="list-style-type: none"> • 108941 The Temple • 127006 South Ealing Road • 168407 Colne Road • 55023 Broadway 	
--	--	--	---	--

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

				<ul style="list-style-type: none"> • 256340 Margeston Crescent • 377201 Summerfield • 277208 Merry Hill Centre • 122033 Manor Way • 103002 Chingford Station Road • 57912 Langley Green • 190002 Upper Clapton • 138002 Plaistow • 170306 Busy Lane • 56005 Neasden • 57002 Rushmore Road • 124002 Church Road • 156020 Bilton Road • 178909 Dover Road • 207026 Beacontree Heath • 188004 High Road 358 • 233523 Tredworth • 165313 Durham Road • 217323 Elford Grove • 342201 Springfield • 364340 Bolton-On-Dearne • 392422 Woodsend Road • 282611 Barry Road • 333406 Digmoor • 231832 Uddingston • 540201 Lea Village • 232246 Whitmore Reans • 232340 Highfield <p>For these branches:</p> <ul style="list-style-type: none"> • 10 are new entries for w/c 8 June, so will have initial telephone calls made to them by the Branch Analysis and Audit team • 4 have agreements with the Branch Analysis and Audit team that need to be monitored this week • 6 require re-contacting by the Branch Analysis and Audit team 	
--	--	--	--	---	--

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

				<ul style="list-style-type: none"> • 1 has an outstanding transaction correction that was sent last week that will reduce the generated cash position of the branch • 4 have visits planned this week from the Audit team • 3 are with the Area Managers, 4 have agreements with the Branch Analysis and Audit team that need to be monitored 	
3.2.2	<p>Internal Audit Charter:</p> <p>Johann Appel was asked to update the the Charter and circulate to the Committee to specifically call out examples of cash and cyber security.</p>	JA	July	This has been completed.	Recommend for closure
3.4	<p>Committee Evaluation Report:</p> <p>Annual Legal Risk Report (non GLO) to be produced quarterly or on a half yearly basis.</p>	BF/DP	July	The Annual Legal Risk Report will be presented in September and March as part of the meeting programme.	Recommend for closure
4.	<p>Co-operation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy:</p> <p>The Committee agreed that the wording needed to be double and triple checked before final approval in consideration of how the policy might be perceived if it were to be made public.</p>	BF	July	The Policy has been recently reviewed by GE and further updates regarding wording have been requested prior to Board approval.	Open
5.2	<p>Selling Regulated Products</p> <p>Ken McCall requested that Jonathan Hill speak to McKinsey as a matter of priority about this Action Plan.</p>	JH	July	<p>Update from Andrew Kingham (Head of Network) 20/7/20:</p> <p>Initial scoping of the requirements necessary to improve the current conformance score has been completed that we have found that along with revised training of and communication to postmasters, we</p>	Open

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

				<p>will need to implement three key systematic changes as well.</p> <p>These changes will include:</p> <ul style="list-style-type: none"> • Improved postmaster journeys on the Point of Sales system, that will drive an improved sales conversations. • Local printing changes for ID8000 labels • Implementing a “customer confirmation” step onto the PIN pad <p>The first stage of project set up is now being requested through our formal governance process, the PRB (Project Review Board), to gain funding approval. It is expected to have this approval by the end of July 2020.</p> <p>Once complete, resources for a project team will be allocated to this work, and requests to commence changes to IT systems can be made. In addition, documentation of any training, support and communication to postmasters will also be planned, after which we will be able to provide completion dates to this forum.</p>	
5.3	An independent review of suspense accounts as part of the GLO work	AC/BF	July	An update is being presented to ARC 27/07/20 and has been discussed at RCC 13/07/20.	Recommend end for closure
5.3	An independent review of stamps and whether any GLO implications	AC/BF	July	This is being presented at Board 27/07/2020.	Recommend end for closure
5.3	CBRE performance issue	AC	July	In progress. The remedial actions have been completed and a dialogue with the supplier is underway.	Open
5.3	Work ongoing to validate historical final salaries for the defined benefit pension scheme	AC	July	An update is being presented to ARC 27/07/20 and has been discussed at RCC 13/07/20.	Recommend end for closure

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

8.1.2	Risk: dashboards generated from Archer be presented to ARC	MB	July	These have been included as part of the risk report for ARC 27/07/2020.	Recommend end for closure
8.1.4	RMG POL talks: there did not need to be a change in approach (following the departure of Royal Mail CEO but this would be monitored).	NF/AC	Ongoing	In progress and will revert separately to the Board	Recommend end for closure
8.2	Compliance: PSD2 - The business had confirmation from Fujitsu that a solution will be in place by August 2020. A draft letter was being prepared to the FCA to update them on the latest position.	JH	July	The FCA responded on 29 th June 2020 to thank us for our clear letter and confirm it is happy with the approach.	Recommend end for closure
8.2	European Electronic Communications Code: The Department of Culture, Media and Sport (DCMS) were seeking to hold businesses to a compliance deadline of 21 December 2020. However, Ofcom was working to clarify timings and push the deadline into next year. This was a watching brief.	JH	July	Compliance and the Telecoms Team are commencing work now to understand how long the changes will take and the costs involved.	Open
8.3	Internal Audit: Postmaster Onboarding – Has feedback been sought from newly on-boarded postmasters?	JA	July	A targeted survey has not been done, but there is a robust process whereby feedback (complaints etc.) is recorded and acted upon (we reviewed this as part of the audit and did not identify any adverse feedback).	Recommend end for closure
8.3	Internal Audit: Vetting / Fit & Proper - JA to confirm the periods for re-checking of staff.	JA	July	There is currently no requirement to re-vet employees other than for Supply Chain staff. JA can confirm that Supply Chain staff are re-vetted every three years in line with Security Industry Authority licencing requirements. For all other staff, there is an audit action for Julie Thomas and HR to consider implementing a process for periodic re-vetting of key individuals (due end August). For Fit & Proper, JA	Recommend end for closure

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

				can confirm that all employees subject to HMRC regulations undergo re-certification on an annual basis.	
9.3	Annual Report and Accounts: The Chair highlighted that the Committee needed to understand how the revenue and adjustments tie into agent remuneration and requested assurance on this matter.	PwC	June	An updated paper on revenue and adjustments was presented to the Committee in June.	Recommend for closure
10.	PCI-DSS & Cyber Security: Jeff Smyth to share the presentation from the CEO to CEO session with Ingencio with the Committee.	JS	ASAP		Open
10.1.2	PCI-DSS & Cyber Security: Fujitsu relationship - A broader piece of work was being undertaken to look at the Fujitsu relationship across the business, particularly in relation to PCI – DSS, Telco and Freedom of Information Requests. The work would be brought to the May and June Boards.	JS	May/June		Open
10.2	Cyber Security: Maturity - An update on the actual achievement, re-baseline of the target level maturity and plans for any gap remediation would be shared with the Committee once the audit was complete.	TJ	July	An update is being presented to ARC 27/07/2020	Recommend for closure
24 March 2020					
5. Minutes and Matters Arising					
5.2	An update on Successfactors was included under any other business	Lisa Cherry	July 2020	<u>Update: 15/07/2020</u> – a deep dive will be presented in September. A paper will be presented to the July ARC meeting.	Open

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

	but a fuller review would come back to the July 2020 ARC meeting.		ARC meeting		
7. 2020/21 Internal Audit Plan					
7.	We needed a revised plan that reflected the current environment and the top five priorities. We also needed a monthly update from Deloitte on the external environment, including risks and the approach other companies were taking to managing their risks and running their businesses	Johann Appel/ Deloitte		Ongoing. Deloitte will provide a monthly update to the ARC.	Open
12. Selling Regulated Products in the Branch Network					
12.	Mails Dangerous Goods compliance: It was AGREED that an action plan would be created and provided as part of the next Compliance Report to the ARC.	Amanda Jones/ Andy Kingham	19 May 2020 ARC Meeting July 2020 ARC Meeting	<u>Update from 19/05/2020:</u> An update on Dangerous Mails Action plan is provided as part of the May Compliance Report. However, it had been agreed that an Action Plan would be created and this was still in train. Jonathan Hill explained that the team was working on a plan to enable Pin Pad validation for mails contents and in the meantime, training was being undertaken and Area Managers were monitoring compliance with training requirements as a priority. Ken McCall requested that Jonathan Hill speak to McKinsey as a matter of priority about this Action Plan.	Open
28 January 2020					
4. PCI-DSS and Cyber Security					
4.3	The Committee urged the management team to press for compliance pre-Christmas, even if roll out was delayed until after the Christmas trading period. He did feel more assured with the joint effort/approach to compliance.	NR	March	<u>Update 15/07/2020:</u> CEO level talks have now taken place. Further CEO level talks are expected to take place in April 2020.	Recommend end for closure
4.4	It was AGREED monthly progress reports (signed by Ingenico's CEO)	JS	On going	<u>Update 15/07/2020:</u> Updates are being circulated to ARC.	Recommend end for closure

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

	would be provided to the Committee.			This has been agreed by Ingenico, to commence circulation.	
25 November 2019					
5. Contract Management					
5.3	MB/NR That the full accountability matrix based on the RACI principles should be compiled and presented to the Committee. It was discussed and agreed that this should be extended to all functions (not just contract management). The Operational Risk team will assist NR.	MB/NR	March 2020	<p><u>Update 15/07/2020:</u> New management structure and accountabilities now agreed. 3 line of defence model being implemented and supported by KRIs using existing KPI data. Update to ARC in September 2020.</p> <p>An updated matrix will be presented once NR confirms his new management structure and accountabilities.</p> <p>Central Risk have refreshed the Post Office enterprise risks such that there are now 14 enterprise risks and 55 linked intermediate business risks. Each of these risks has a designated GE or GE-1 owner in line with the latest Post Office organisational structure. Ownership will be change controlled as individual risks emerge, are managed and then recede. Specific ownership will be included as part of the Archer Dashboard reporting suite going forward.</p>	Recomm end for closure
5.3	Auditors to provide examples of best practice for contracts management.		March 2020		Open
23 September 2019					
6. Transformation Office Changes					
6.5	Consider the prioritisation of the change portfolio at the POL Board	DZ	January 2020	Added to To be included in January Board agenda.	Recomm end for closure
29 January 2019					
6. Money Laundering Reporting Officer (MLRO) Annual Report					

**Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 15 July 2020**

6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	Nick Boden /Sally Smith	Ongoing	Update 15/07/2020 Included in compliance report. Ongoing until project close. Item included on ARC agenda.	Recommend for closure
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	Rob Houghton / Mick Mitchell	May 2019	Update: 15/07/2020 Included in PCI-DSS Cyber Security reports. Standing agenda item until further notice. Ongoing. Item included on ARC forward agenda.	Recommend for closure
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	Exec	May 2019 July 2019	<u>Update: 15/07/2020</u> Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Recommend for closure



**POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE**

Minutes of a Risk and Compliance Committee (“RCC”) meeting held via Microsoft Teams on 13 July 2020 at 14:00

3.4

- | | | | | |
|-----------------------|--|---|------------------------|--|
| Present: | Alisdair Cameron (Chair) (AC) | Group Chief Financial Officer | | |
| | Ben Foat (BF) | Group General Counsel | | |
| | Amanda Jones (AJ) | Group Retail and Franchise Network Director, Interim | | |
| | Lisa Cherry (LC) | Group Chief People Officer. | | |
| | Jeff Smyth (JS) | Group Chief Information Officer, Interim | | |
| | Julie Thomas (JT) | Operations Director | | |
| | Chrysanthy Pispinis (CP) | Post Office Money Director, Post Office | | |
| | In Attendance: | Johann Appel (JA) | Head of Internal Audit | |
| | | Mark Baldock (MB) | Head of Risk | |
| | | Jonathan Hill (JH) | Compliance Director | |
| Tom Lee (TL) | | Head of Finance, Financial Accounting and Controls | | |
| David Parry (DP) | | Senior Assistant Company Secretary | | |
| Tony Jowett (TJ) | | Chief Information Security Officer | Item 4 | |
| Joseph Moussalli (JM) | | Programme Manager, Project Managers and PMOs | Item 4 | |
| Rob Wilkins (RW) | | Cloud Services Director, MI, Data Strategy & Analytics | Item 4 | |
| Tim Armit (TA) | | Business Continuity Manager | Item 5 | |
| Tim Perkins (TP) | | Head of Security, Safety & Loss Prevention, Loss Prevention | Item 7 | |
| Apologies | Maxine Cross (MC) | Head of Reward & Pensions, Reward & Pensions | Item 8 | |
| | Sarah I Gray (SIG) | Group Legal Director | Item 9 | |
| | Andy Kingham (AK) | Head of Network, Retail Network | Item 10 | |
| | Sally Smith (SS) | Head of Financial Crime | Item 10 | |
| | Nick Read, Group CEO | | | |
| | Owen Woodley, Group Chief Commercial Officer | | | |

1.	Welcome and Conflicts of Interest	Actions
	The Chair opened the meeting and advised that all papers would be taken as read. No conflicts of interest were declared.	
2.	Minutes and Action Lists	
2.1	The minutes of the RCC meeting held 6 May 2020 were APPROVED .	
2.2	<p>Progress on completion of actions as shown on the action log was NOTED. The following action updates were provided:</p> <ul style="list-style-type: none"> - Action 3.3 from 6 May 2020 relating to COVID-19 wider enterprise risk statement had been discussed at June’s GE and could therefore be closed. - Action 3.9 from 6 May 2020 relating to Belfast Data Centre Exist and move to the Cloud is being discussed at July’s GE meeting and could therefore be closed. - Action 3.10 from 6 May 2020 relating to Whistleblowing can be closed. An update is being presented at this RCC meeting. - Action 3.15 from 6 May 2020 relating to the fit and proper policy would remain open until LC and JT had discussed HR involvement in the policy. - Action 3.15 from 6 May 2020 relating to Internal Audit Reviews could be closed. Updates have been provided to ARC. - Action 3.16 from 6 May 2020 relating to Status of Internal Audit actions could be closed. Updates have been provided to ARC and actions continue to be tracked. - Action 3.3 from 14 March 2020 related to an IA Cyber Security audit in FRES would remain open. No audit had been completed as yet. - Action 6.6 from 14 March 2020 related to Annual Legal Risk Report 2019/20 would remain open. The item has been added to the programme cycle for September and March. 	<p>To do:</p> <p>LC/JT</p> <p>JA/TJ</p>

Strictly Confidential

Page 1 of 6



3.4

	<ul style="list-style-type: none"> - Action 10.6 from 14 January 2020 relating to supervisory HMRC meetings between BF and POL's new supervisor would remain open until the meeting had been completed. HMRC are not conducting meetings at present following COVID but SS would chase a meeting date. - Action 3.2 from 7 November 2019 relating to supplier contracts out of governance (SSK) remained open. Funding was on hold until October. - Action 5.3 from 7 November 2019 relating to a Cyber Security major incident test remained open. A test would still required. - All other recommended actions for closure were closed. 	SS JS/TJ
3.	Combined Risk, Compliance and Audit Update	
	Risk	
3.1	<p>MB presented the risk report.</p> <p>Focus since the last meeting had been on embedding the three lines of defence model into POL. Archer had been populated with 453 clearly identified risks and owners (15 overarching enterprise risks, 70 linked intermediate risks and 350 subsidiary local risks) and work has also been completed to assimilate the POL Covid-19 risk identification and management activity into the wider enterprise risk.</p>	
3.2	Approval has been received from GE to refresh the corporate risk appetite statements (last reviewed in 2015) and to establish a supporting set of key risk indicators using existing KPI data. A pilot is underway to plot a set of KRIs for with Operations/Legal, IT and Finance.	
3.3	<p>The Committee noted the following key enterprise risks remain:</p> <ul style="list-style-type: none"> • Commercial – POL not an attractive business proposition due to complex/confusing products, new products considered cost ineffective and difficult to scale. • Covid-19 – the risk to business employees/postmasters and the business remain, particularly in light of reduced footfall/trading on the high street. • Financial – concern that funding is insufficient and costs uncontrolled in the short/medium/long term leading to the inability to deliver strategic objectives. • Legal – POL unable to comply with legislative and regulatory changes, resulting in fines, lost revenue, reputational and customer damage. It was noted that legal and regulatory updates would be provided to RCC to avoid this. • Technology – POL is heavily reliant on key 3rd IT parties that is difficult to influence and has an ageing IT infrastructure. There is concern that the disaster recovery regime is ineffective. • Operational – low quality branch network locations and remuneration package for agents may impact revenue for POL and PostMasters. <p>Change Portfolio remains at Amber.</p>	
	Compliance	
3.4	<p>JH presented the compliance report with the following points noted.</p> <p>Telecoms: JH noted that POL continues to prioritise fault repairs for vulnerable customers and to honour the commitments made to DCMS. Weekly updates continue to be requested by Ofcom who have now resumed their monitoring and enforcement programme.</p> <p>The Committee raised concern with POL's inability to effectively deal with S136 and 137 information requests, in terms of the accuracy of information provided to the regulator and the reliance on 3rd party providers for information without carrying out sufficient checks.</p> <p>The Chair requested that more a comprehensive response programme be developed to reduce the possibility of being penalised.</p>	Action: TL/BF/JH
3.5	<p>Fairness: JH reported (Ofcom) would be reporting on fairness in early 2021 and that POL is considered (by the regulator) to have a high number of customers considered 'vulnerable' i.e. those who have been paying higher prices than customers in contract for more than 2-3 years.</p> <p>The Committee challenged the Telco team to reduce the number of 'vulnerable customers' and to revert to the Committee with a statement/plan for September.</p>	Action MS



3.4

3.6	<p>GLO/Freedom of Information Requests: JH remarked resource has been stretched responding to Historic Shortfall Scheme, related/linked FOI requests (55 as at 24.06.2020) and CCRC requests. The sensitivity/complex nature of the FOI requests has required external legal support, as well as approval from the GLO Steerco and notification to UKGI before release.</p>	
3.5	<p>Belfast Data Centre Exist and move to the Cloud: JH noted that data migration from the Belfast Data Centre is planned for eight weeks' time, and that an approach has been agreed between IT, Legal and Compliance.</p> <p>This approach enables POL to deploy a contractual and operational solution that eradicates the need for approval from upstream clients where personal data may be processed outside of the EEA. A compliant solution inside POL's Risk Appetite has been identified and is under development.</p> <p>JS noted that the talks with upstream clients and the short time from for data migration would be challenging.</p>	
3.6	<p>Cookies: JH advised a solution has been built and deployed to meet the Directive 2009/136/EC, (known as the Cookie Law), however the solution does not fully satisfy all regulator (ICO) consents.</p> <p>The Data Protection and legal teams are reviewing the implications to POL following a recent case in Germany where a company used a similar solution to POL's but was deemed to be non-compliant with EU legislation.</p>	
3.7	<p>Financial Crime: there has been a large increase in suspicious activities reports during lockdown, with 930 SARs and 159 investigations in April & May (cf 598 and 84 in April & May 2019). The team is working closely with the banks to understand the reasons for the spike.</p>	
Internal Audit		
3.8	<p>JA presented the IA report.</p> <p>A summary of findings from last year's IA programme (2019/20) noted 171 audit actions across 25 audits in total (cf 271 actions across 24 audits in 2018/19). JA advised the lower number of actions could be attributed to a general improvement in the control environment.</p> <p>Some improvements are required in core controls following system and organisational changes during the year, risk management and governance oversight has slightly decreased, but information, communication and report turnaround has improved.</p> <p>The Chair requested the IA team identify ways to improve core controls.</p> <p>It was AGREED a list of management accountabilities would be circulated to GE and GE-1 members.</p>	<p>Action: JA</p>
3.9	<p>The Committee noted the following audits have been completed since the last ARC meeting (6/5/20):</p> <ul style="list-style-type: none"> • FS Branch Sales (FY20 IA Plan) (Final Report) • CV-19 Programme Assurance - Ph1 Set-up & Governance • Minimum Control Standards – Ph1 Cash Controls • Minimum Control Standards – Ph2 Minimum Control Standards – Ph2 • Cyber Security Maturity Assessment • Effectiveness of Second Line during CV-19 – Ph1. <p>The combined Risk, Compliance and Audit paper was NOTED for onward submission to the ARC.</p>	
4.	PCI-DSS and Cyber Security Update	
PCI-DSS Programme Update		
4.1	<p>JS presented the PCI-DSS update.</p> <p>He reported further funding has been agreed by the Board (26 May 2020 Board meeting) to progress the programme until completion, and that NR and JS had met with Paula Felstead, Ingenico Group CTO. Ingenico had provided a renewed commitment to achieve Vocalink Accreditation by the end of December 2020.</p>	



3.4

	The Banking forum has also been updated with a plan/timetable of key dates for 2021, indicating Pilot and Branch rollout commencing in February 2021. He expects formal PCI DSS accreditation to be achieved by June 2021.	
4.2	<p>The following PCI key risks were discussed:</p> <ul style="list-style-type: none"> Any additional essential changes required to the Fujitsu /Ingenico software would impact the planned timeline. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis there are no further changes. Concern that POCa payments cannot be routed through Vocalink within the timescales. The team is working to identify a solution. Concern that Santander cannot migrate payments to route through Vocalink within the timescales. The team is working closely with Santander. 	
4.3	<p>The Chair noted the progress made, but requested the report should clearly identify what progress has been made, the areas completed, those on track or not, and those that remain outstanding. Technical jargon should be avoided.</p> <p>The PCI-DSS Programme Update was NOTED for onward submission to the ARC.</p>	
Cyber Security		
4.4	<p>TJ presented the Cyber Security update.</p> <p>Cyber Security Maturity: good progress has been made with the Deloitte cyber security maturity assessment and a report from Deloitte is expected in July detailing detailed actions for further mature Cyber controls. In the interim, Internal Audit has worked with Deloitte to provide an overarching report giving key recommendations and maturity assessments.</p> <p>Compared to last year, TJ believes maturity is more secure, and that focus should be on developing a cyber security strategy as the business and IT strategies unfold.</p>	
4.5	<p>Covid-19: TJ noted that during the pandemic, phishing traffic had increased but that SPAM-based mail attacks now appear to have returned to normal levels. The team has completed a targeted phishing simulation to raise awareness within POL.</p>	
Joiners Movers Leavers (JML)		
4.6	<p>TJ presented the JML report.</p> <p>JML remains a key focus for the team. A draft reference model has been developed identifying the role and accountability of each department in the JML process, helping to reduce single points of failure.</p> <p>Good progress has been made enhancing the integrity of the links between Success Factors, Microsoft Identity Manager and Active Directory which controls access administration and the project is expected to be completed in August 2020.</p>	
4.7	<p>Regarding third party access to JML, although the team conducts audits, POL remains reliant upon suppliers being honest. A move to a cloud (such as Belfast Exit project) presents an opportunity for greater oversight and control.</p>	
4.8	<p>The Chair noted the progress made, but remarked ARC would question why the project had not been completed, as well as the lack of control over 3rd party access.</p> <p>The Cyber Security Update and JML report was NOTED for onward submission to the ARC.</p>	
5. Business Continuity Update and Business Continuity Policy		
5.1	<p>TA presented the Business Continuity update.</p> <p>A complete failure of Horizon (no strategy has been developed for large scale failure) remains POL's key risk, but the current approach to resilience remains effective.</p>	
5.2	<p>Covid19 has demonstrated that POL can run effectively via home working for an unlimited period of time, and the ability to maintain call centres with home working including supporting a third party POCA call centre, means a solution is now being considered and explored. The 'Post Office on Wheels' (deployed for contingency purposes) has proved effective during the pandemic, however plans should be developed to mitigate against a second Covid wave.</p>	
Business Continuity Policy		



3.4

5.3	TA advised there have been no material changes to the policy since last year and that it remains suitable for purpose.	
5.4	The Business Continuity update and Policy were NOTED for onward submission to the ARC.	
6. GDPR Update		
6.1	JH presented the GDPR update. The team has now completed a review of contracts not previously remediated or de-scoped during the original GDPR remediation programme, identifying 7 key contracts as high risk including: <ul style="list-style-type: none"> • CWU • Unite • Fujitsu Telecoms • Global Payments • OH Assist • RAPP • Selenity. 	
6.2	Work is underway to support the contract owners, however the Committee remains concerned that other high risk contracts may be identified following programme completion. The GDPR Update paper was NOTED for onward submission to the ARC.	
7. Suspense Accounts		
7.1	BF and TP presented the Suspense Accounts report. BF explained that KPMG had been commissioned to review whether POL has profited from money held in suspense accounts, following longstanding allegations pre and post GLO.	
7.2	A review of current practices has now been completed and identified four suspense accounts currently in operation. These suspense accounts contain money that is: <ol style="list-style-type: none"> (1) Either not taken to a profit and loss account; or (2) Relates to unmatched transactions due to customers (not Postmasters); or (3) Relates to surpluses rather than shortfalls. 	
7.3	TP remarked that no money has been identified as being taken for profit, and that the team would be implementing KPMG's suggested recommendations over the course of the year. It was noted the review did not cover the historical operation of the suspense accounts, which the Chair requested be investigated.	Action: TJ
7.4	The paper was NOTED for onward submission to the ARC.	
8. Pensions Assurance		
8.1	MC presented the Pensions Assurance paper. She advised that ahead of the POL purchasing its share of the Royal Mail Pension, the project had identified a number of material systemic errors in the provision of pensionable data provided by POL to the Royal Mail Pensions Service Centre.	
8.2	These errors are predominantly linked to the incorrect configuration of Success Factors, and the misinterpretation of how promotional increases are treated in the pension terms. Willis Towers Watson (POL's actuarial advisers) has been engaged to help identify the extent of these errors, and to assist with mitigation to avoid future error. An internal audit has also been commissioned to understand why this has not been previously identified, and to ensure that any lessons are learnt.	
8.3	BF highlighted to the Committee that the POL's directors may wish to make a report to the regulator, and that they would be entitled to obtain their own independent legal advice which could be arranged through the legal team. The Committee discussed and recognised the potential for future litigation and regulatory fines (which should not be underestimated), and noted that the legal advice received had strongly indicated that no report should be made at this stage, until the scale of issue was known. MC was reminded that the potential for litigation should not be underestimated.	
8.4	The paper was NOTED for onward submission to the ARC.	

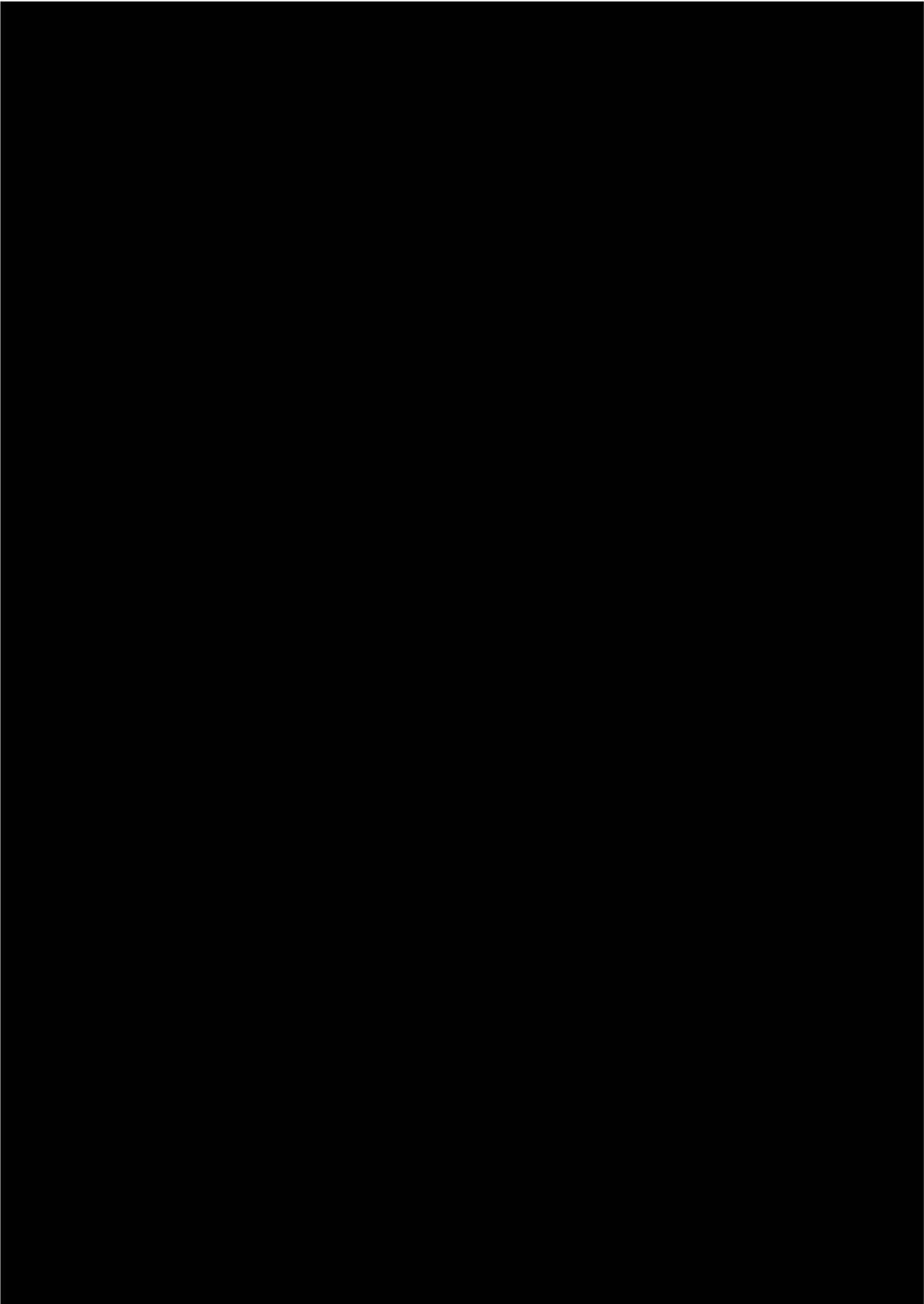
Strictly Confidential

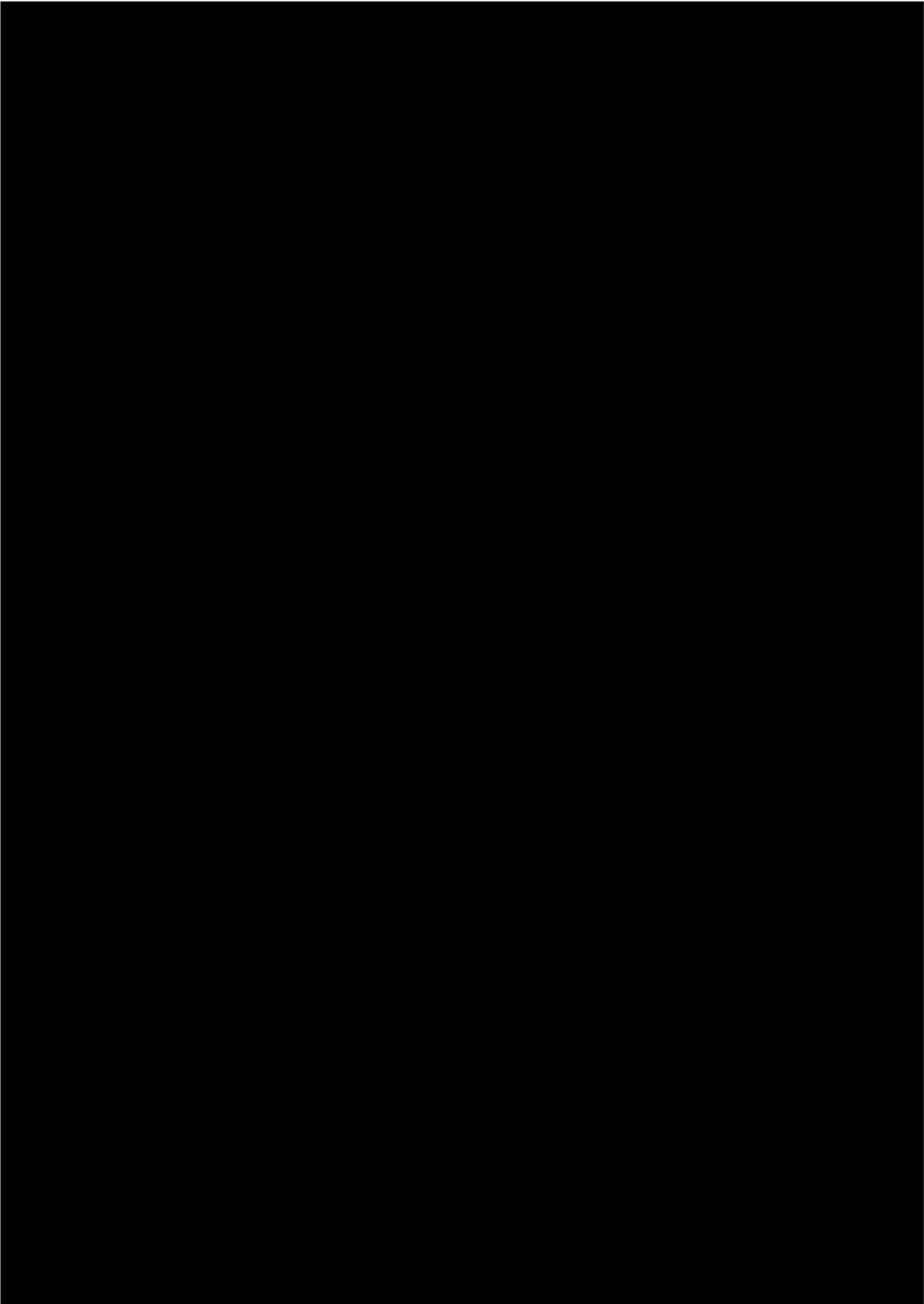
Page 5 of 6

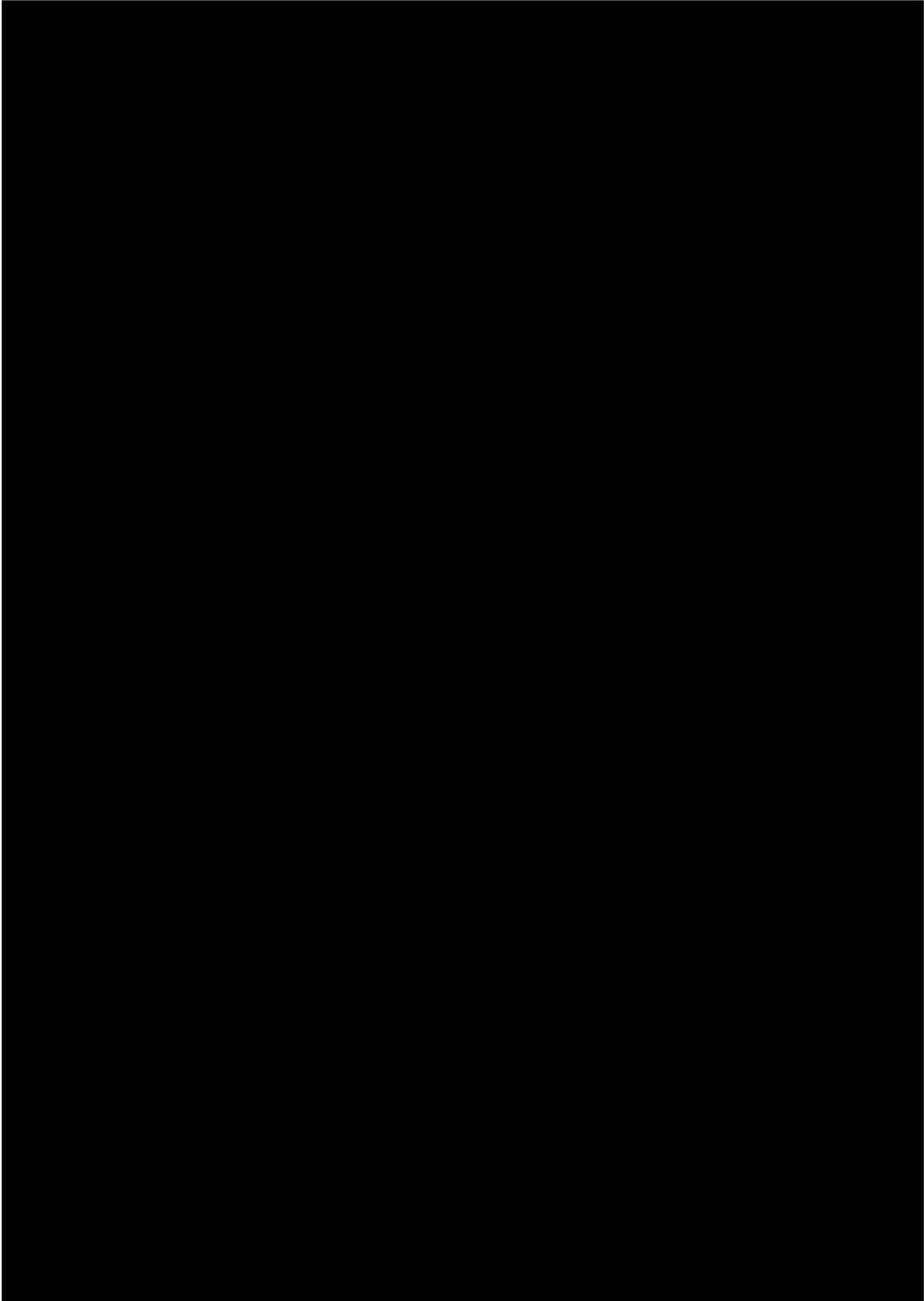


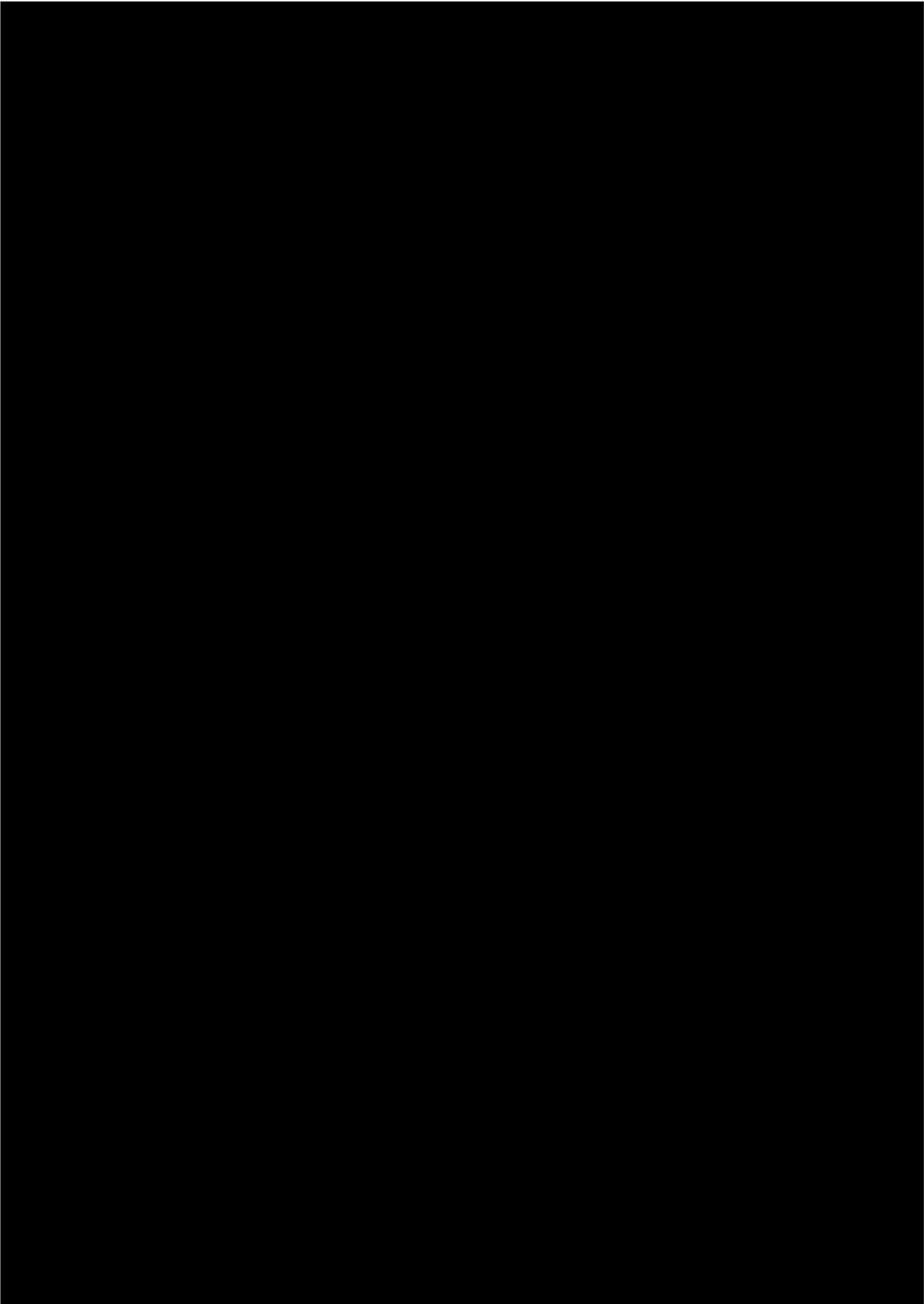
3.4

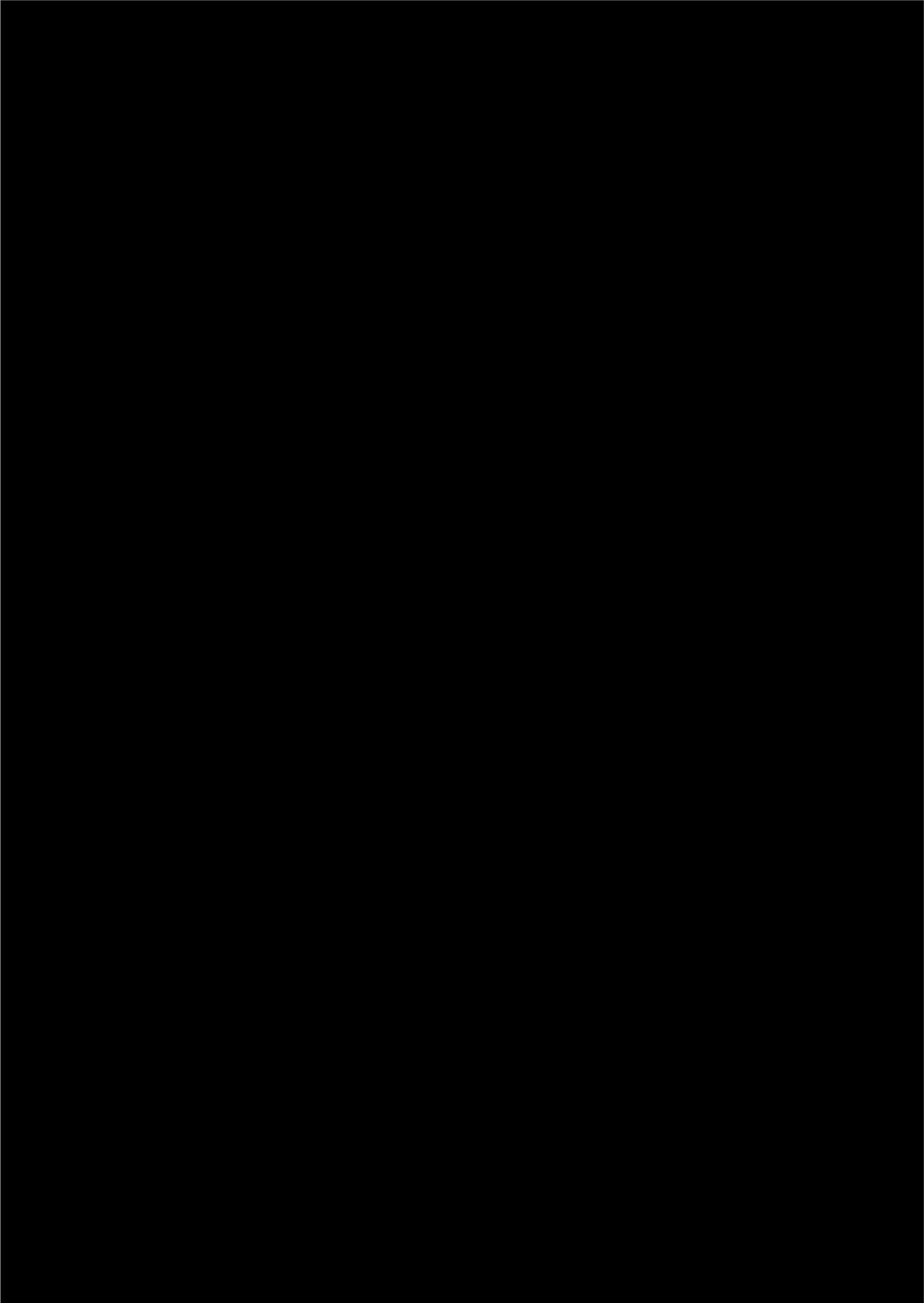
9.	Law and Trends Update	
9.1	SIG presented the Law and Trends update paper.	
9.2	She explained the purpose of the paper was to highlight any future legislation and or regulation that may impact POL, bringing the following to the Committee's attention: <ul style="list-style-type: none"> • Covid 19 Employment Legislation Updates. • ATM Additional Business Rates Update. • Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations. 	
9.3	Covid-19 Employment Legislation Updates: there has been a recent flurry of legislative changes to react/mitigate against Covid-19. The Coronavirus Act 2020 (effective 25 March 2020) introduces emergency powers to handle the COVID-19 pandemic. Working groups continue to review and monitor guidance to ensure POL is compliant.	
9.4	ATM Additional Business Rates Update: a recent UK Supreme Court case has ruled that ATM facilities do not need to be assessed separately for business rates. POL has approximately 53 ATMS where claims can be made via an online system, however, only the occupier of the site can make the claim. In this instance, BOI would have to make the claim for POL backdated to 31 March 2018.	
9.5	Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations: public sector websites have a legal duty to make sure their websites meet accessibility requirements by 23 September 2020. Mobile apps are expected to be compliant by 23 June 2021. The digital innovation team believed POL's website was compliant and work was ongoing to meet the mobile applications compliance by the June 2021 deadline.	
9.6	The paper was NOTED for onward submission to the ARC.	
10.	Policies for Approval:	
	The following policies were NOTED for onward submission to the ARC: <ul style="list-style-type: none"> • Modern Slavery Statement: AK provided a more robust training regime had been implemented and that there was a greater understanding in the network about slavery/exploitation. JT highlighted the positive impact the branch support guide had provided to branches to highlight any issues of modern slavery and where to report these. • Anti-Bribery and Corruption Policy • Whistleblowing Policy • Financial Crime Policy • Anti -Money Laundering and Counter Terrorist Financing Policy • Document Retention Policy • Procurement Policy. 	
11.	Review of draft Audit, Risk and Compliance Committee meeting agenda for 27 July 2020	
	The draft ARC agenda for 27 July was NOTED.	
12.	Any other Business	
	There was no other business.	

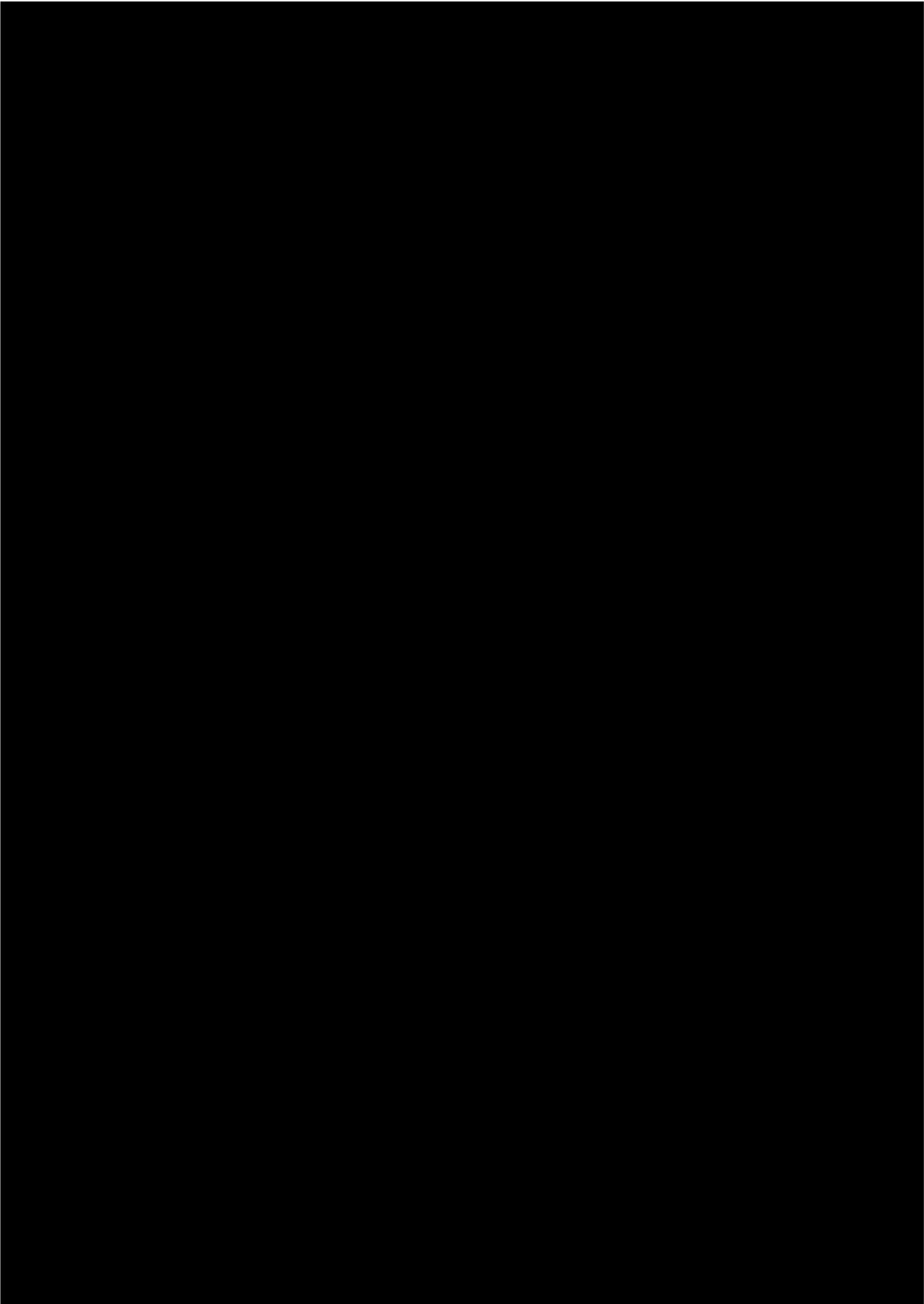


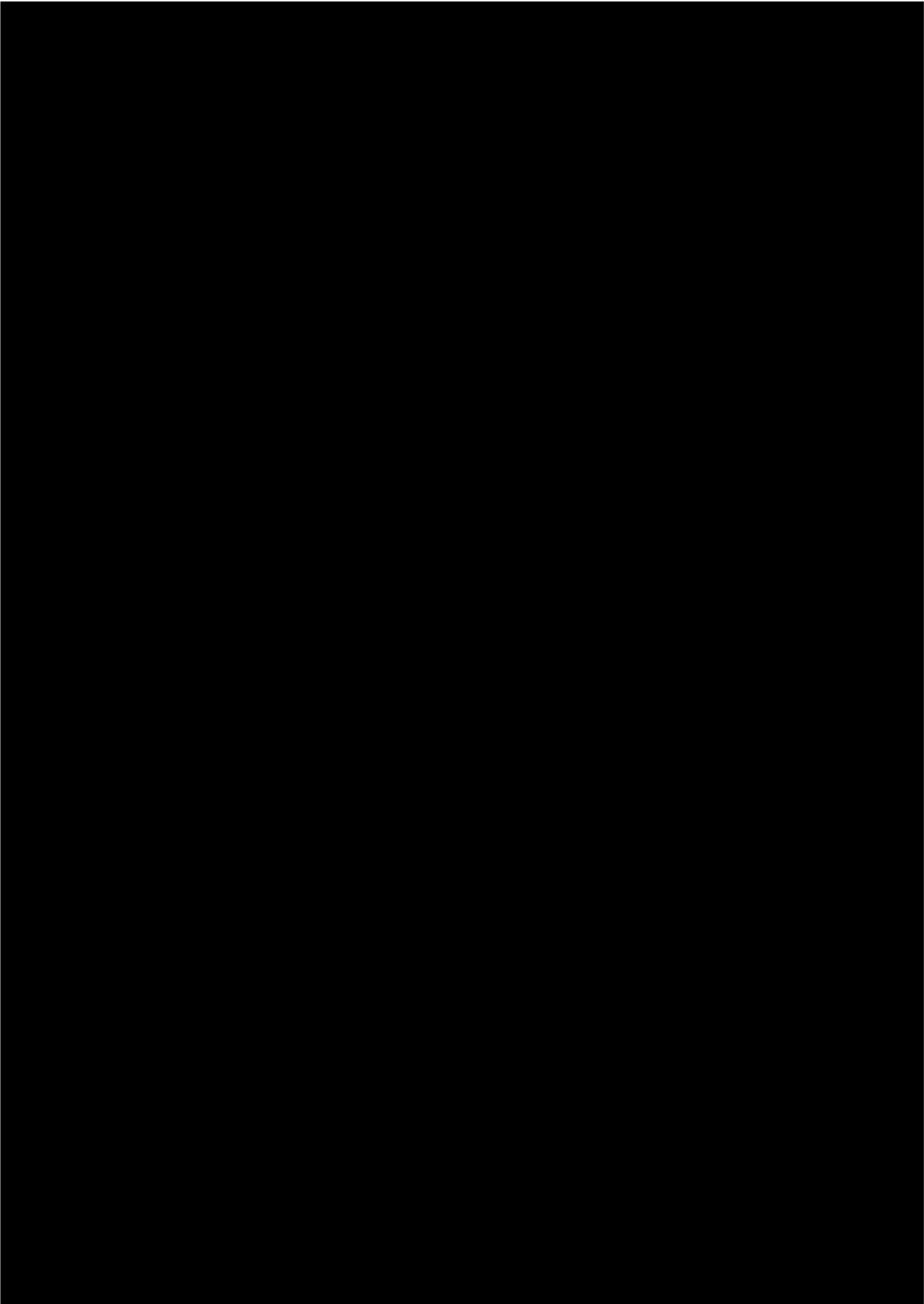


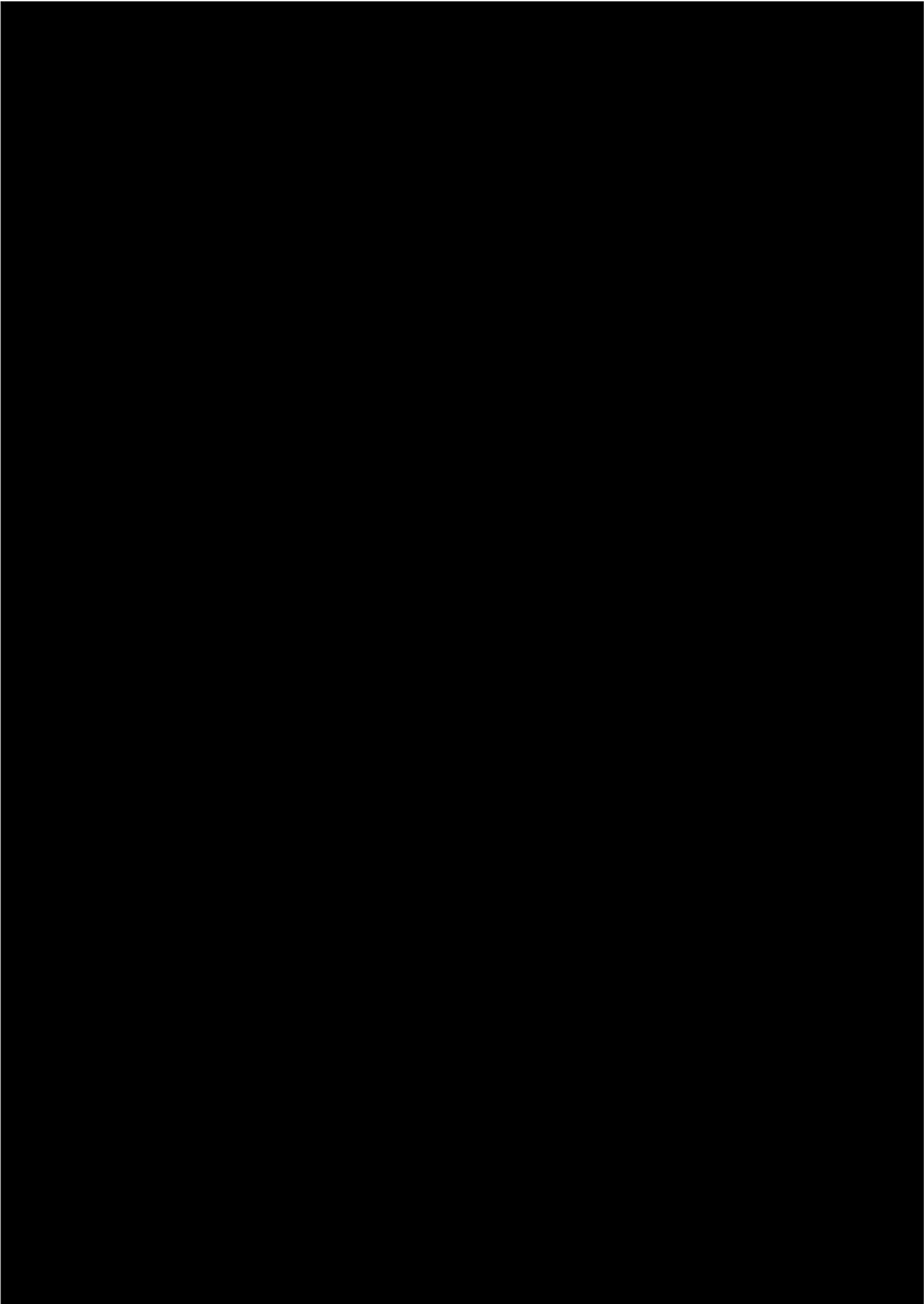


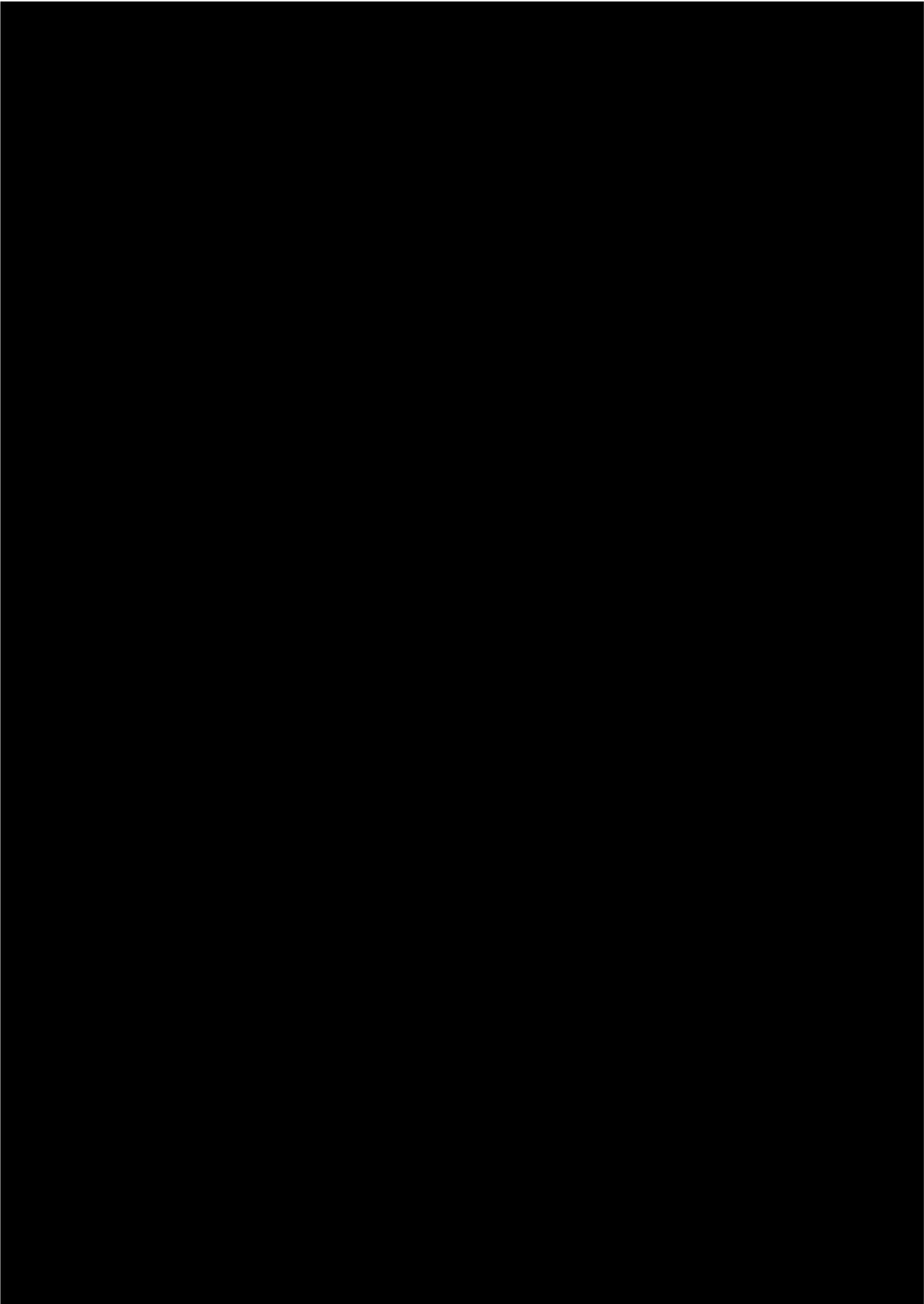


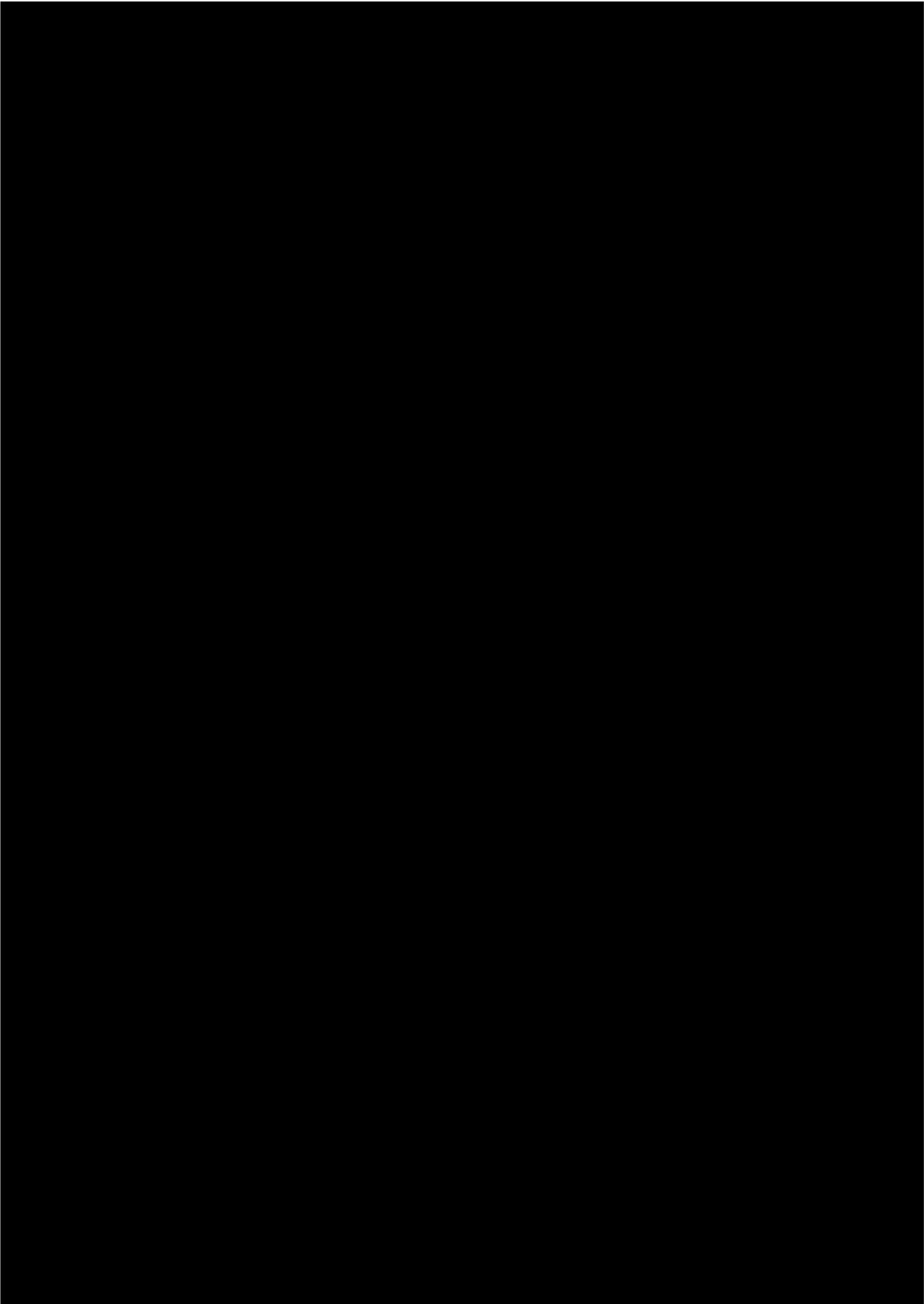


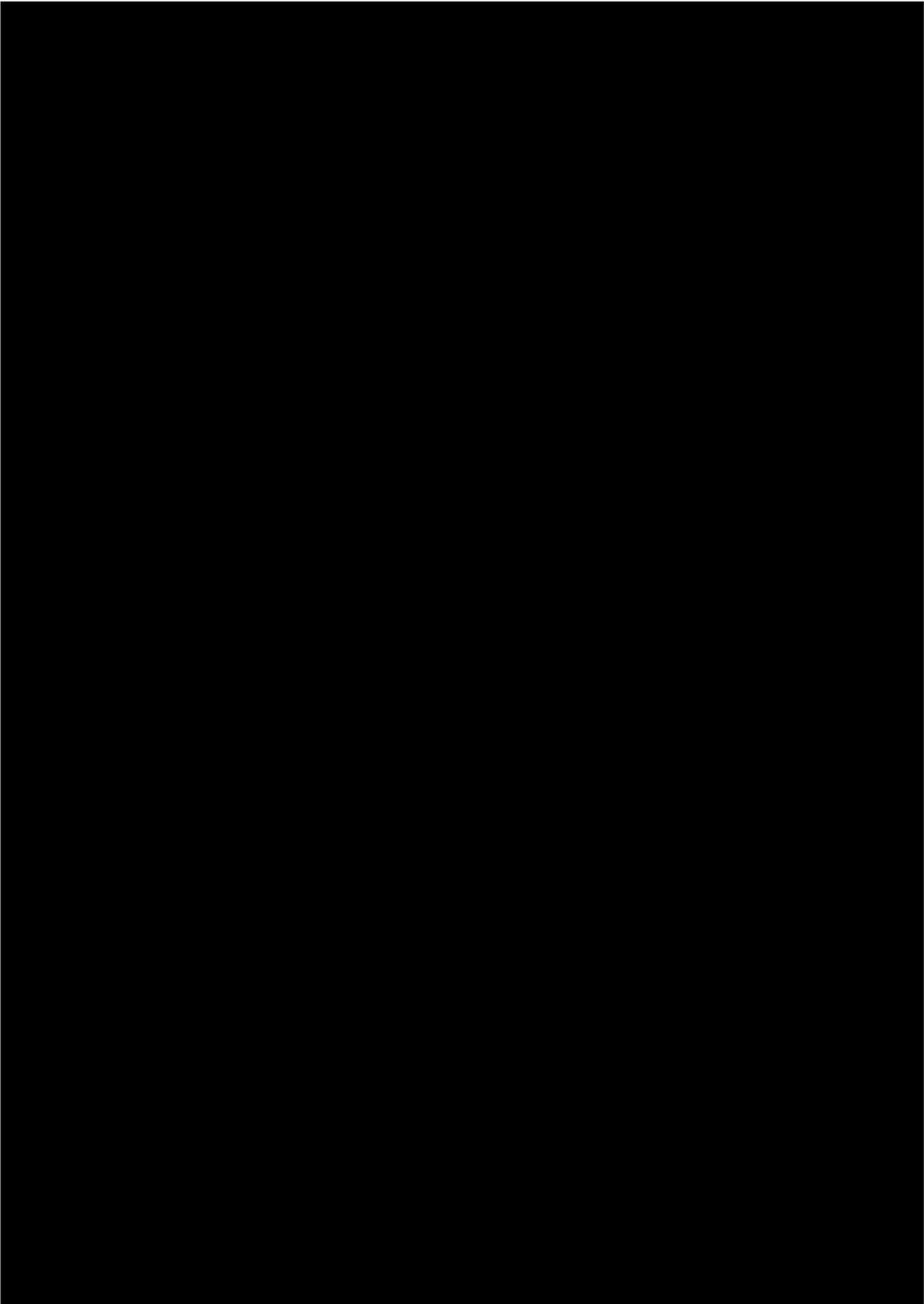


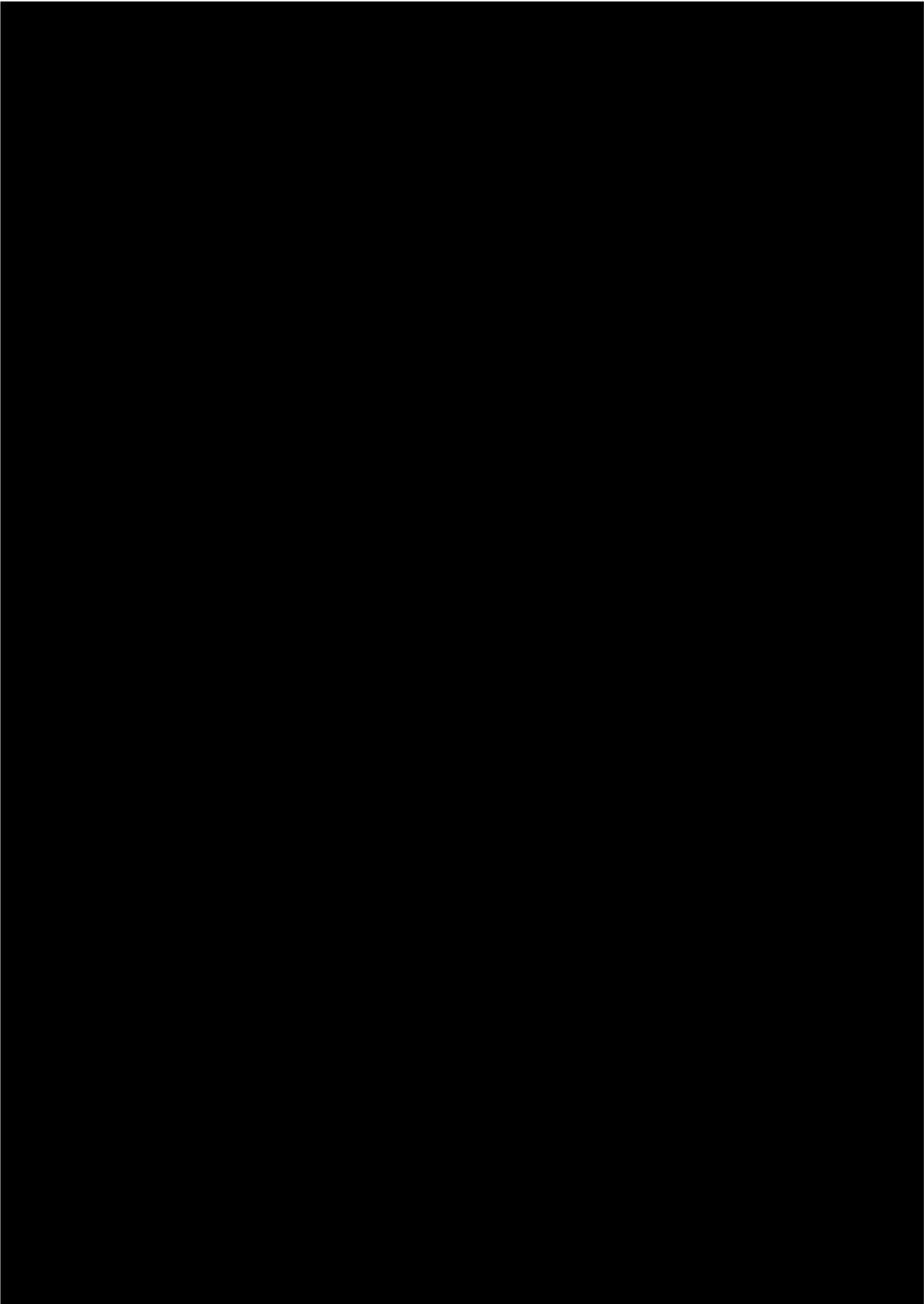


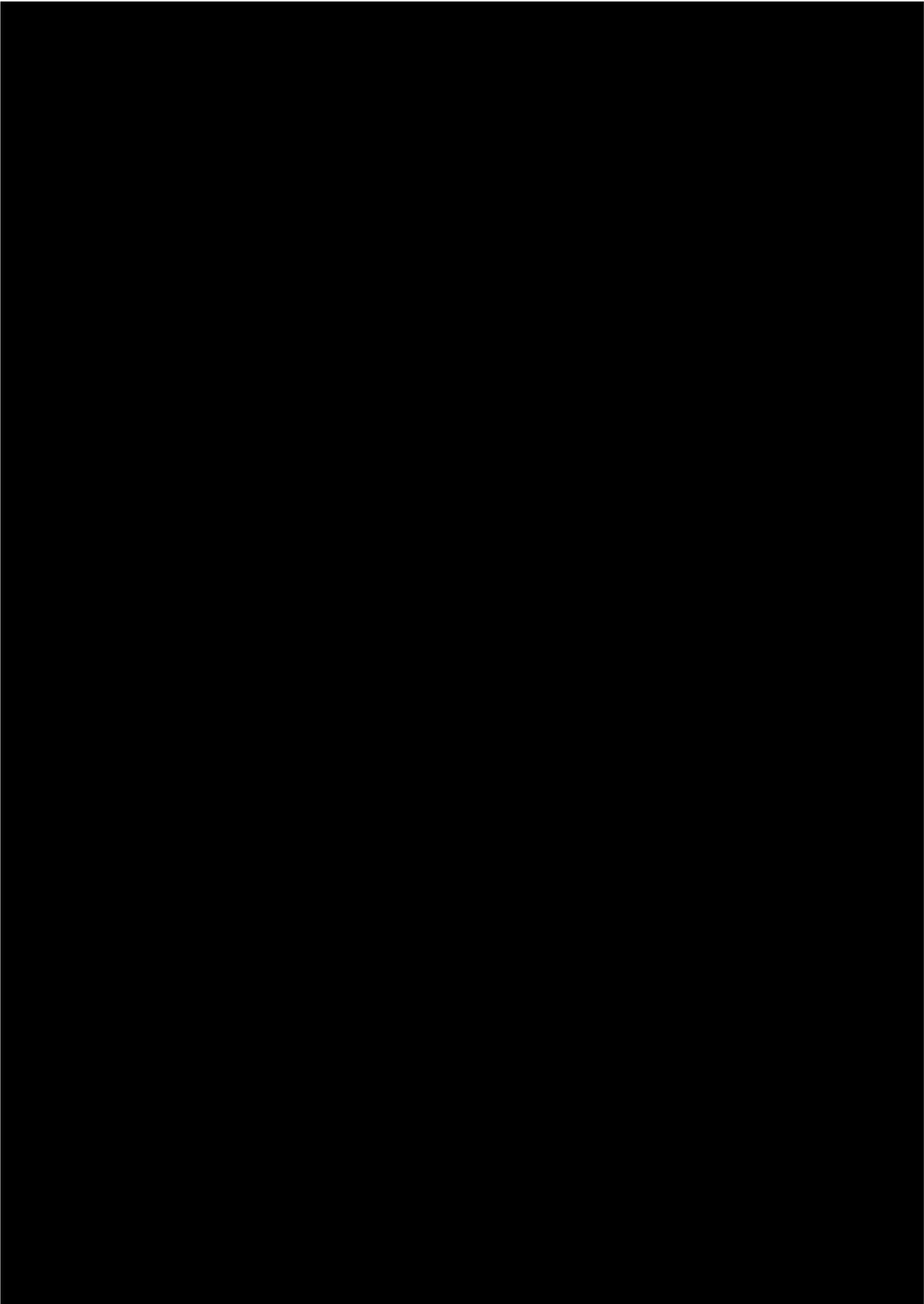


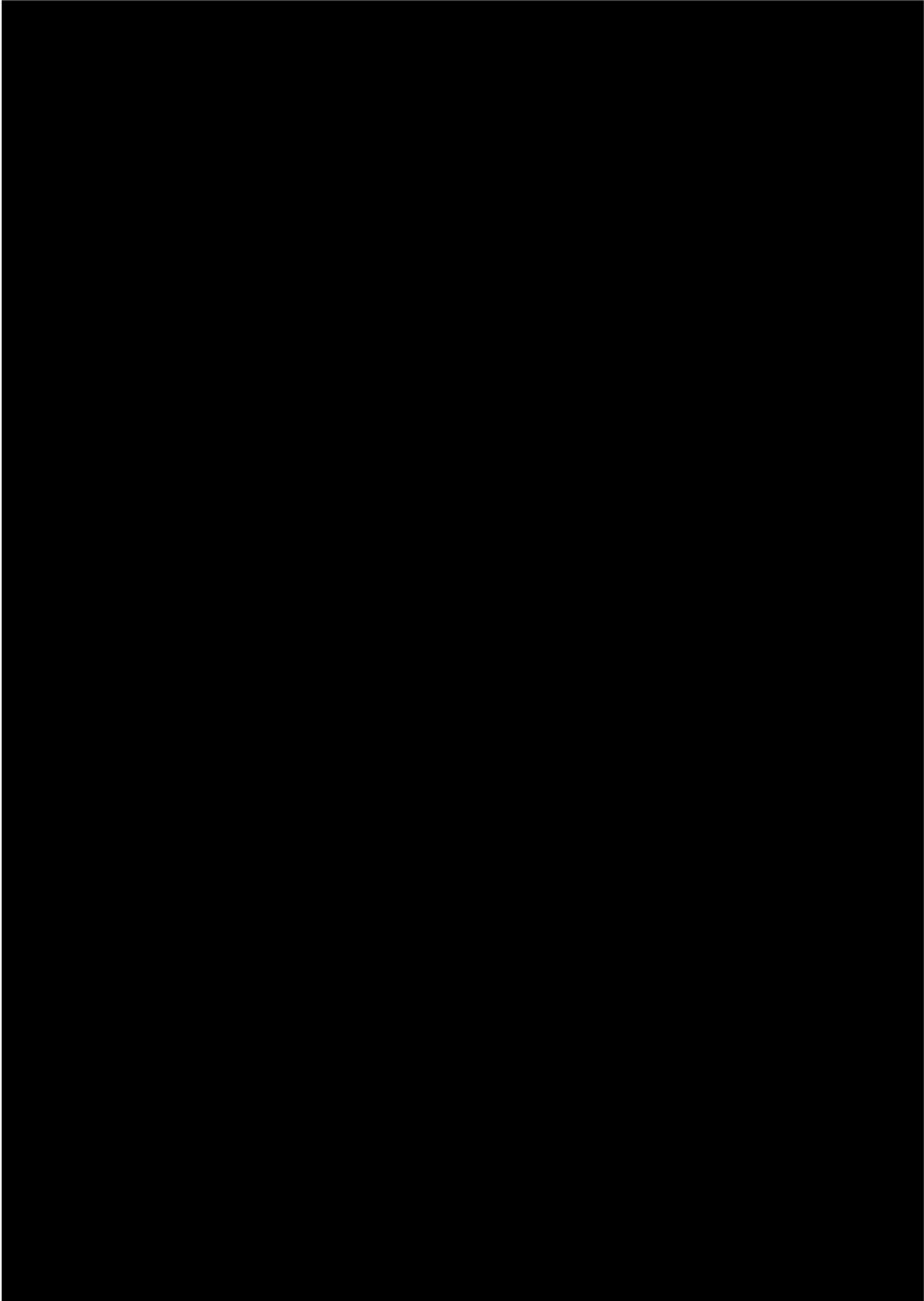


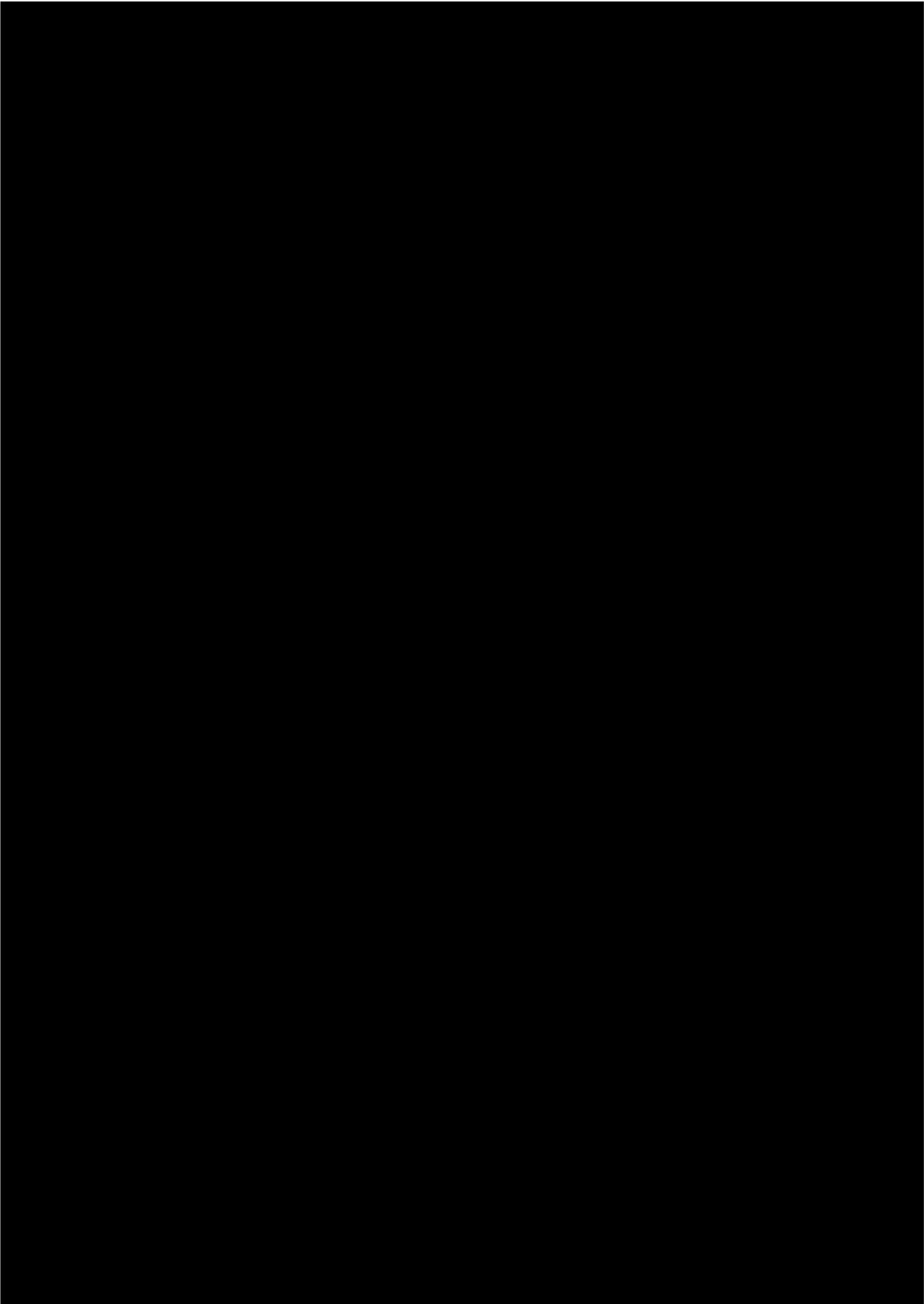


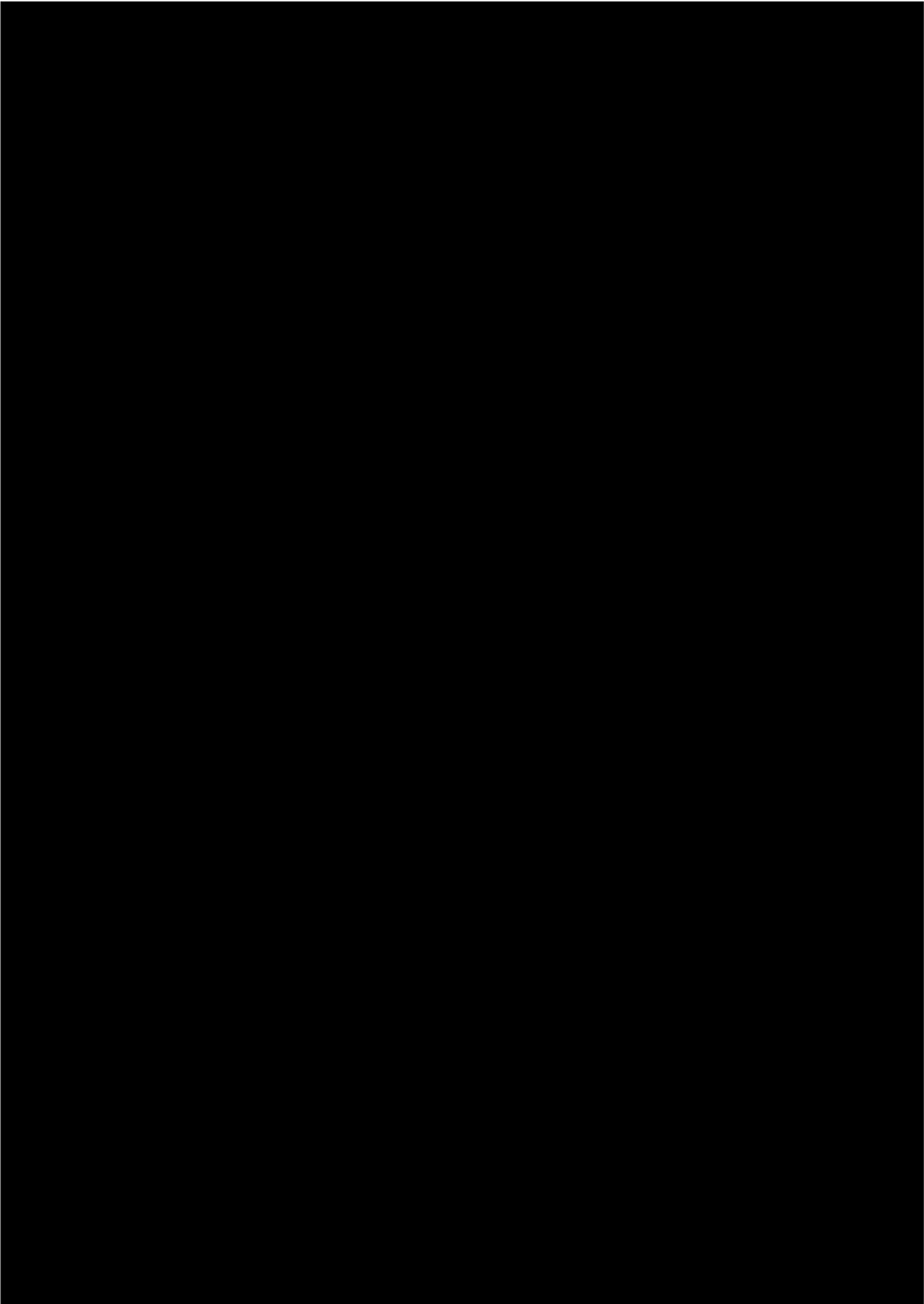














POST OFFICE LIMITED

AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	The Current Operation of Suspense Accounts	Meeting Date:	27 July 2020
Author:	Mark Underwood, Tom Lee & Tim Perkins	Sponsor:	Ben Foat & Alisdair Cameron

5

Input Sought:

The ARC is asked to **note**:

- The findings from KPMG's review of Post Office's current operation suspense accounts.

The ARC is asked to **approve** the recommended approach:

- Whereby KPMG are instructed to explore whether it is possible to perform the same independent review, but for Post Office's historical operation of suspense accounts.

Previous Governance Oversight

- Post GLO Settlement Programme SteerCo of 1 July 2020
- RCC 13 July 2020

Executive Summary

1. Allegations continue to be made that Post Office may have recovered sums from Postmasters (including through civil and criminal proceedings) which were not 'real losses' to Post Office as they were housed in suspense accounts and taken to profit by Post Office.
2. KPMG were instructed to review Post Office's current operation of suspense accounts. Although their findings include a number of points to consider in terms of how Post Office could enhance best practice. In summary, given the robust and transparent investigations process that is undertaken, these suspense accounts should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit. This is because sums housed in suspense accounts are either:
 - not taken to a profit and loss account; or
 - relate to unmatched transactions due to customers (not postmasters); or
 - relate to surpluses rather than shortfalls.
3. BAU investigations and the Historical Shortfall Scheme provide mechanisms whereby shortfalls can be investigated and/or resolved. However, this is unlikely to satisfy Post Office's detractors.
4. Thus, and at a cost of c£47k, it is recommended that the ARC approve instructing KPMG to explore whether it is possible to perform the same type of independent review, but for Post Office's historical operation of suspense accounts.
5. The ARC should note that any documentation which is produced and findings made, may be disclosable as part of Post Office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical

1

Confidential



practices, in both a civil and criminal context and in the context of any relevant investigation or inquiry.

Questions addressed

1. What is a suspense account? What allegations have been made in respect of how Post office operates suspense accounts?
2. What assurance does KPMG's review give Post Office? What were the findings?
3. What options exist to Post Office for managing any historical and future suspense account related claims?
4. What further work could KPMG perform over the historical operation of suspense accounts? How much would this cost? What are the limitations and risks?

5

Report

History & Context

1. Post office uses suspense accounts:
 - To house branch discrepancies arising as part of the normal course of trading and which need to be cleared at the period end (either surplus or deficit).
 - To house surpluses arising from Postmasters where the Postmaster does not agree the surplus is due back to them.
 - To temporarily hold differences in payments moving between Post Office and its clients, where the client and Post Office's view of what is payable or receivable differ. Differences are investigated but in some cases neither Post Office, the client, nor the branch are able to determine the identity of the customer who performed the transaction in question or the specifics of the transaction. For example, Post Office may not be able to determine the details of the bank account to be credited. In such situations, and following enquiries with branches, unresolved differences are moved to Post Office customer creditor suspense account. Such discrepancies are held in its suspense account to give time for customers and other parties to put forward more information to explain what has happened.
2. A long standing assertion, made by applicants to the Complaint Review & Mediation Scheme, Claimants in the GLO, and by Lord Arbuthnot is that:
 - Post Office operates one or more suspense accounts in which it holds unattributed surpluses including those generated from branch accounts;
 - After a period of time, such unattributed surpluses are credited to Post Office's profits; and
 - Post Office therefore has recovered (through civil or even criminal proceedings) sums from Postmasters which were not real losses to Post Office, as they were housed in suspense accounts and ultimately taken to profit by Post Office.
3. These allegations were first made in the context of the Complaint Review & Mediation Scheme¹. Second Sight's² final report, published in 2015, claimed they had been informed that at each year end, substantial unreconciled balances existed on many individual suspense accounts and that these unreconciled balances for the 2014 financial year were approximately £96 million in respect of Bank of Ireland ATMs and approximately £66 million

¹ 'Project 'Sparrow' which, broadly speaking ran from 26 August 2013 – 01 February 2016.

² The firm of independent forensic accountants instructed to investigate each of the applicants cases accepted into the Scheme



in respect of Santander. They said that *"these unmatched balances represent transactions from individual branches that occurred in the preceding 6 months"* and they *"...remain concerned that these balances may include transactions that ultimately should be credited back to individual branch accounts"*.

4. In its 'Reply' to the Second Sight Report, Post Office stated that Second Sight had misunderstood the information provided by Post Office. The balances of £96m and £66m were taken from routine trading balances yet to be settled with other organisations at a particular month end. In other words, they represented amounts due to other parties, not amounts that were unreconciled and which may be due to Postmasters.
5. Second Sight were also provided with details of the credits released from Post Office's suspense accounts to profit for the period 2008 to 2013. As there was a 3 year retention period – no amounts at that time had been released for the years 12/13 and 13/14. The total gross credits released from suspense to profit from 2007/8 onwards was as follows:

Years released to profit	Value
2010/11	£612,000
2011/12	£207,000
2012/13	£234,000
2013/14	£104,000
2014/15 (YTD at the point provided)	£8,000

6. In its reply to Second Sight, Post Office stated that amounts should be considered within the overall context of Post Office performing around 2.5 billion transactions per annum, with a combined value in the order of £60bn. The amount of unresolved credits that end up in Post Office's P&L (at the time) was therefore less than 0.001% of all transactions (by value) undertaken by branches.
7. Allegations continue to be made in respect of Post Office's suspense accounts. In February 2020 Lord Arbuthnot wrote to Nick Read. In Nick's response, he committed to better understanding how Post Office operates its suspense accounts. Nevertheless, in the House of Lords on 18 June 2020, Lord Arbuthnot complained that the Terms of Reference for the recently announced 'Independent Review into the Post Office Horizon IT System and Trials' do not *"say anything about the likelihood of the Post Office improperly making a profit from the sub-postmasters, or about the suspense accounts"*.

KPMG's Suspense Account Review

8. KPMG were instructed to review how Post Office currently operates its suspense accounts. The scope of this review was as follows:
 - Confirm the number of relevant suspense accounts operated by Post Office into which sums are placed which could, theoretically, relate to discrepancies at a branch level and from which any unmatched sums may be taken into a Profit and Loss (P&L) account.
 - For these accounts, assess whether how they are operated reflects the associated documentation and best practice.



- Identify whether there are any gaps / challenges within existing processes which could result in risk to Post Office and or Postmasters.
- Assess whether the current resolution criteria adopted by Post Office for dealing with discrepancies appears 'fair and reasonable' to both Post Office and Postmasters, based upon KPMG's understanding of best practice.
- Comment on any further work that Post Office might want to consider.

KPMG's Findings

9. KPMG identified 4 relevant suspense accounts which are currently operated by Post Office; details of which are provided within the table on the following page. In summary, given the robust and transparent investigations process that is undertaken, these suspense accounts should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit.

5

10. This is because sums housed in suspense accounts:

- are either not taken to a profit and loss account; or
- relate to unmatched transactions due to customers (not Postmasters); or
- relate to surpluses rather than shortfalls.

11. For completeness and although purely hypothetical, included at **Annex 1** is a worked example for how a postmaster could repay a shortfall which Post Office has or eventually could take to profit via a suspense account. Post Office is not aware of any examples of this having taken place and it requires, for example:

- a Postmaster not following process;
- refunding a customer, prior to an investigation taking place and without contacting Post Office;
- not recording the refund on Horizon; and
- not recalling the refund during the subsequent investigation.

Owing to its nature therefore, it would be extremely difficult if not impossible for Post Office to prevent.

Account	Description	Houses Deficits and or Surpluses?	Postmaster Affecting?	Are unmatched sums taken to P&L?	KPMG Findings Summary
Branch Snapshot. Current Balance: £355,204	This is a holding account within branch accounts which allows Postmasters to investigate discrepancies that have arisen within their branch without the need to recognise and potentially settle the amount at their trading period end.	Deficits and Surpluses potentially due to Postmasters	Yes	No. These accounts relate to discrepancies identified by Postmasters and which result in a Postmaster either repaying (deficit) or being repaid (surplus) amounts.	Branch Deficits KPMG's assessment is that Post Office are moving towards best practice. There is an established, robust and timely investigation and resolution process which is undertaken in conjunction with Postmasters and the development of a tailored training course encompasses the key aspects of best practice. In addition, the level of monitoring and oversight is robust ensuring there are no unauthorised transactions and aged balances do not build up.
Local Suspense. Current Balance: £0	Branch discrepancies arising at the period end are posted to this account. The balance on this account must be cleared before the branch can complete their period end roll over. Depending on the value of the discrepancy, the balance is either made good through the Postmaster putting cash into the office (if less than £150) or can be 'settled centrally' (if over £150) meaning the balance is moved in to the Postmaster's personal account in the Group Ledger. Discrepancies can be investigated after they are made good or posted to the Postmaster's personal account in the GL			Resolution of these discrepancies is either in cash or via Postmaster's personal accounts in the Group Ledger.	Whilst operational documentation provides Post Office with a clear audit trail, there is a lack of formal detailed process documents and inconsistencies between documented and actual practices. Branch Surpluses Policy and procedures are unclear and Postmasters are not routinely informed when surpluses arise on their personal accounts in the Group Ledger. The timeliness of repayment is dependent upon the value of the surplus and is in direct contrast to the branch deficit policy. There is a currently a backlog into investigations of surpluses and monitoring of branch surpluses is inconsistent.
Agent Creditor. Current Balance: £17k	This account holds surplus discrepancies which Post Office believes are due to Postmasters, but that Postmasters dispute being due to them.	Surpluses potentially due to Postmasters	Yes	Yes. This accounts house surpluses from which unmatched items can be released to the Post Office P&L account after 5 years. However, as this account relates to <u>surpluses</u> which are disputed by the Postmaster (as opposed to	Formal policies in place regarding when amounts can be released to the P&L account. Though operational policies are clearly understood, they are informal and not yet fully documented.





Account	Description	Houses Deficits and or Surpluses?	Postmaster Affecting?	Are unmatched sums taken to P&L?	KPMG Findings Summary
				Post Office) any improper operation should not result in Post Office potentially pursuing Postmasters for monies it had already or could eventually take to profit	
<p>Customer Creditor: Current Balance: £3.5m</p>	<p>This account holds amounts repaid to Post Office from third parties due to issues identifying who the money is owed to.</p> <p>Third parties include Santander, MoneyGram and Camelot customers.</p> <p>Amounts are held in this account, pending inquiry from the customer.</p>	<p>Surpluses potentially due to customers</p>	<p>No. These monies relate to <u>customers</u> who cannot be traced due to inaccurate data.</p>	<p>Yes. This account houses surpluses from which unmatched items can be released to the Post Office P&L account after 6 years or earlier where specific policy is to do so.</p> <p>However, as this account relates to unmatched sums potentially due to customers (as opposed to Postmasters) any improper operation should not result in Post Office potentially pursuing Postmasters for monies it had already or could eventually take to profit.</p>	<p>An established level of best practice in respect of documentation, monitoring and resolution.</p> <p>A good level of operational documentation provides a clear audit trail and monitoring ensures there are no unauthorised transactions to or from the account.</p> <p>All amounts posted in this account are investigated with the relevant branch prior to being posted in this account.</p> <p>No evidence that amounts posted to this account would relate to branch discrepancies which were previously repaid by a Postmaster.</p>



Recommendations Included within the KPMG Review

12. The KPMG report includes a number of points to consider in terms of how Post Office could improve its operation of suspense accounts to enhance best practice. These include:
- Implementing and documenting policies and procedures including details of ownership, format, content and version control for all relevant suspense accounts.
 - Ensuring all processes are adequately documented and that policies are consistently applied within the documentation.
 - Implementing an overarching branch discrepancy process document linking all relevant policies and processes.
 - Formalising the reporting and review by senior management of suspense accounts and investigation outcome metrics.
 - Undertaking a review of the branch deficits written off centrally to identify whether any Postmasters are regularly benefitting from the policy.
 - Reviewing the policy and process for branch surpluses with specific focus on:
 - i. Communicating surpluses to postmasters.
 - ii. Repayment timescales not being determined by value.
 - iii. Timeliness of investigation process.
 - iv. Aligning the branch deficit and branch surplus policies and expectations.
 - Implementing a process to address the current backlog that has arisen in the investigation of branch surpluses and the resolution of old branch surpluses that are in dispute to ensure:
 - i. Repayments are made in a timely manner; and
 - ii. Where appropriate, amounts are moved into the Agent Creditor Account.
13. All recommendations are being taken forward, and will be implemented through BAU over the course of the 20/21 financial year.

Next Steps

14. Although the KPMG report gives Post Office assurance that its current operation of suspense accounts should not result in sums being pursued from Postmasters which Post Office has already or could also take to profit via a suspense account, the scope of the review did not include Post Office's historical practices.
15. If a historical error, in relation to the operation of suspense accounts, was to adversely affect a branch, this would almost certainly manifest itself as a shortfall. The Historical Shortfall Scheme provides a mechanism for shortfall claims to be investigated. The only caveat to this is if their claim relates to a period of time for which the branch in question was operating on HNGA. This is because HNGA related claims are ineligible for the Scheme.
16. However, any such 'suspense account related claim' which relates to a period during which HNGA was in operation at the branch in question would still manifest itself as a shortfall and can therefore be investigated through current BAU processes (which KPMG have found to be transparent and robust).



-
17. Nevertheless, this is unlikely to satisfy Post Office's detractors and the allegations will continue. As such it is recommended that the ARC approve instructing KPMG to explore whether it is possible to perform the same independent review, but for Post Office's historical operation of suspense accounts. It may not be possible, owing to the timeframes involved (2000 – 2019), key personnel no longer being in the business and documentation being destroyed in line with retention schedules (prior to legal holds being in place). KPMG has provided a cost estimate of £47k to complete this work.
18. If it is possible, the ARC should note that any documentation which is produced and findings made, may be disclosable as part of Post Office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical practices, in both a civil and criminal context and in the context of any future investigation or inquiry.

5



Annex 1 – Theoretical example for how a Postmaster could repay a shortfall which Post Office has or eventually could take to profit via a suspense account³:

Step	Customer balance	Branch balance	Postmaster balance	POL balance	Bank balance
A customer makes a £10 deposit in branch.	£0	£0	£0	£0	+£10
The customer complains the deposit has not been received in the associated banking account. By way of an example, this could be as a result of the Postmaster incorrectly recording the account details on Horizon.	-£10	£0	£0	£0	+£10
The Postmaster chooses to refund the customer £10, without recording it on Horizon	£0	-£10	£0	£0	+£10
The bank refunds £10 to Post Office.	£0	-£10	£0	+£10	£0
Prior to Post Office moving £10 to its Customer Creditor Account, Post Office investigates with the branch in question any sums originating from transactions performed within that branch. If the Postmaster does not recall refunding the customer - the £10 would be moved to the Customer Creditor Account.	£0	-£10	£0	+£10	£0
At the end of the trading Period (having still not recalled refunding the customer) the Postmaster chooses to make good the £10 shortfall.	£0	£0	-£10	+£10	£0
If after 6 years the amount remains unmatched, it is released to Post Office's Profit & Loss Account	£0	£0	-£10	+£10	£0
Thus, Post Office has received £10 from the Postmaster but still houses the original £10 within its Customer Creditor Account	£0	£0	-£10	+£10	£0

5

³ For simplicity, this table ignores any applicable transaction fees.



POST OFFICE LIMITED AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	GDPR Contract Remediation	Meeting Date:	27 th July 2020
Author:	Jonathan Hill	Sponsor:	Ben Foat, General Counsel

Input Sought: Noting and Approval

Previous Governance Oversight: RCC 13 July 2020

Executive Summary

1. This paper reports on the outcomes of the new GDPR Contract Remediation project, which took place between December 2019 and the end of June 2020.
2. A new project was approved in November 2019 to close out the contracts that had not been remediated during the original programme. The project was given a £250K budget and was tasked to complete its work by end June 2020. Estimated spend at completion is £118K.
 - a. 243 contracts needing to be remediated were identified initially
 - b. 242 additional contracts, which had been de-scoped during the original GDPR programme were brought back into the project as the de-scoping rationale had not been recorded
3. The new project objectives:
 - a. To remediate the outstanding 243 contracts
 - b. To review the de-scoped 242 contracts to determine if they should remain de-scoped or be remediated

The Committee is asked to:

4. Note the report, and
5. Approve the approach to remediation activity going forward



Project approach

6. Initially, 243 contracts had been identified as still needing remediation. However, no records could be found as to why a further 242 contracts had been de-scoped from the original GDPR programme.
7. In order to ensure GDPR compliance, these additional 242 contracts were brought into the new project until the rationale for de-scoping could be identified and approved.
8. The project was led by Compliance and supported by Legal, with a small project team. All contract remediation activity closure was approved by the Post Office Legal Director, Compliance Director and the DPO.
9. Contracts were prioritised depending on their materiality to Post Office and the GDPR risk. If the counter-party would not engage with Post Office and the contract was deemed to be low risk, then a "Deemed Consent" approach was taken, as approved by the ARC in November 2019.
 - a. Deemed consent will not remove the legal risk but is a pragmatic approach to close out the remediation work.
 - b. Given the changes in the GDPR legislation and the concept of dual accountability the ICO will consider the efforts made by Post Office to remediate the contracts in line with legislation and the failure, by our contracting parties, to engage.
10. If a counter-party taken down the deemed consent route wished to enter into negotiations with Post Office we agreed with their request.

6

Project status

11. All 485 contracts have now been reviewed and actions taken (please see Table 1)
 - a. 272 went through a remediation process and 213 that were originally de-scoped had their status confirmed.
12. Of the 272 that have gone through a remediation process, 24 were returned to the contract owners as other contractual activity with the counter-party was or is about to be underway. All of these will continue to be supported by the Compliance Data Protection Team and Legal as part of normal BAU activity.

These agreements were returned to the business for various reasons:

- a. Contract was due for renewal could be picked up as part of that work
- b. Wider sensitive negotiations were ongoing with the counterparty
- c. Business were looking to amend the contract and it was decided that GDPR remediation could be picked up as part of the amendment
- d. Out of the 24 agreements, seven have been highlighted as high risk:
 - CWU
 - Unite
 - Fujitsu Telecoms
 - Global Payments
 - OH Assist
 - RAPP
 - Selenity



- e. All are being addressed and have support from the Legal team and/or the Data Protection team
- f. Caseworkers from Legal and Compliance will continue to work with the contract owners to see these through to completion.

Table 1

Contracts in Remediation (as at 16.07.2020)	
Contracts identified for remediation	243
Re-scoped contracts returned to remediation	29
Total	272
Remediation completed / de-scoped	
• <i>Remediated</i>	51
o <i>Re-negotiated</i>	29
o <i>Completed through deemed consent</i>	22
• <i>De-scoped following review</i>	189
o <i>Already remediated</i>	26
o <i>Contract to be terminated</i>	4
o <i>Duplicate contract</i>	16
o <i>Licence agreements (no GDPR impact)</i>	102
o <i>No evidence of live contract</i>	8
o <i>No personal data being processed</i>	21
o <i>No longer has POL relationship</i>	11
o <i>GDPR policy under pre-existing agreement</i>	1
Contracts moved to BAU for remediation	24
Contracts still in remediation	8

6

Closing out contracts still in remediation

13. Table 2 sets out the current status of the 8 contracts still going through remediation.

Table 2

Contract	Status	Next Steps	Risk Analysis
Fujitsu	GDPR discussions frustrated by wider contract discussions. FJ is resisting changes and has proposed a reduced liability cap. It has been escalated to POL CIO	Internal discussion took place on the 30.06.2020. JS to raise the outstanding issue with Seniors in FJ. Internal agreement on two of the three outstanding issue was reached which is in line with FJ's position. On the outstanding issue POL and FJ are polarised (Security Measures)	This is High risk to POL, particularly given the data being processed and other matter involving Fujitsu. Remediation of this agreement is critical.

Confidential

3



Experian	No engagement from Experian. Experian claiming Covid-19 issues but also dispute on letters Experian claim sent in 2018	Post Office has escalated this through the contract process. Experian have apologised and committed to expediting.	This is a significant contract that needs to be resolved given the sensitivity of the data being processed. This is a High risk to POL until remediated
Verizon UK Ltd	Verizon and POL do not agree on Verizon to flow down terms to its sub-processors and 3 rd party rights	Meeting happened 16.07.2020 Agreements made on all but one point which will be resolved without delay.	Given the nature of the relationship with Verizon this would be a High Risk activity. However Verizon and POL are now in agreement on outstanding issues so this should be moved to completion very soon and now for determined to be a Medium risk.
Inchcape	Inchcape and POL do not agree on data relationship but resolution now close. Our external lawyers are reviewing the Inchcape mark-up and will provide comments to Inchcape w/c 29.06.20	Expecting confirmation shortly to close	This is Low risk to POL given that agreement has now been reached on the key sticking points.
BT (bill payment)	Lack of engagement from BT following feedback from POL.	Meeting scheduled with BT for W/C 20.07.20. BT now keen to close out.	This contract is commercially significant for POL and given that there are material differences between the parties this would be categorised as High. However given the nature of the personal information processed by POL the risk of sanction from Regulators is Low
Santander (bill payment)	Lack of engagement from Santander. Now re-engaged with a proposal from Santander to follow Payout terms	POL agrees in principle with Santanders proposal. Expected to close out shortly	Low risk given the low level personal information processed through this contract. Principles are now agreed
SSE Electricity (bill payment)	Internal SSE governance issue following OVO acquisition of SSE bill payment business needing novation.	GDPR terms agreed and contract should be executed once internal SSE issues closed [ETA mid-July]	The threat of regulatory intervention fro this is Low risk



NCR	Lack of NCR engagement since mark-up sent to them. Expect anything outstanding can be quickly resolved	Escalated to Pol and NCR contract owners to push for response. NCR further stonewalling – Compliance recommend moving to Contract Dispute stage.	Given the nature of the personal data being processed this is of Low risk to POL
-----	--	---	---

14. It is proposed to continue closing out these contracts using resources from Legal and Compliance working alongside the contract owners. Project management resource has ended as it is been reassigned to other projects. The activity will continue to be tracked by Compliance. The Committee is asked to approve this approach.

6

Jonathan Hill
Compliance Director
16th July 2020



POST OFFICE LIMITED ARC REPORT

Title:	PCI DSS Compliance	Meeting Date:	27 th July 2020
Author:	Joseph Moussalli, PCI DSS Programme Manager	Sponsor:	Jeff Smyth, Interim Group Chief Information Officer

Input Sought: For Noting

ARC is requested to note:

What programme progress has been made during the last reporting period?
What are the key risks?

Previous Governance Oversight

ARC has requested a rolling update on PCI-DSS programme progress.

Executive Summary

The programme consists of 2 core delivery streams:

1. The Point-to-Point Encryption (P2PE) workstream, which encrypts retail and banking transactions from the Pin Entry Device (PED) to a PCI compliant zone in Ingenico before onward processing to Global Payments (retail transactions) or VocaLink (banking transactions).
2. The Target Operating Model (TOM) workstream which addresses use of PCI data by POL in processes outside of the transactions occurring at the PED.

The P2PE workstream is on track to deliver Vocalink accreditation of the retail & banking software by January 2020. This activity is followed by a final round of testing and branch piloting activity which is on track to complete by March 2021. After the pilot activity is completed, the solution will be progressively rolled out across all branches with a full rollout and formal accreditation being completed by June 2021. The team is continuing to refine the branch deployment strategy and seek additional improvement in the overall deployment timetable.

The TOM workstream has identified 7 areas where changes to systems and processes are required to achieve PCI compliance. The activity required to address each of these areas has been planned and included in the recently submitted, revised business case.

Key updates in the last period:

- Board approval for a total funding request of £15.8m to deliver the full scope of work. This includes the additional £7.2m required to deliver the complete scope of work required to deliver PCI accreditation.
- The Change Work Order (CWO) covering the scope work to deliver the P2PE solution has been signed off by all 3 parties (POL, Fujitsu & Ingenico) and includes a number of Key Milestones with contracted delivery dates.
- The 1st Key Milestone, the interface specification between the Horizon Counter and the Ingenico Software, has been delivered. The 2nd Key Milestone, an Ingenico demonstration of a banking Balance Enquiry transaction was provided on 17th July 2020.

Confidential

1

8.1



- The upgrade of the Pin Entry Device (PED) to branches restarted on 1st July and is currently planned to complete in September. This had been put on hold due to restrictions put in place during COVID lockdown.
- The solution to obfuscate PCI data on counter screens and receipts has been tested in the Model Office.

Questions addressed

1. What has been the progress since the programme last presented in May 2020?
2. What are the key risks on the programme?

Report

1. What has been the progress since the programme last presented in May 2020?

IT workstream

- The tripartite CWO to deliver the P2PE solution has been signed off through formal governance. The work order includes a number of critical milestones intended to give POL progressive assurance of technical progress of full solution delivery.
- Progress continues in the delivery of the banking solution and Ingenico have delivered the 1st key milestone and that they are on track to deliver the 2nd key milestone in July.
- Ingenico completed the development of the software to support retail transactions and testing is underway with Global Payments. Formal accreditation of the retail part of the solution is on track to be ready for pilot on 23rd October 2020.
- PED Upgrade (firmware upgrade and installation of EMV and banking transaction keys): Completed 78% (19,182 of 24,500 PEDs) of the rollout across POL estate. Deployment was paused on 25th March due to Covid-19 and has just re-started on 1st July 2020. This work is now due to complete in September '20 with no impact to the critical path.
- Good progress has been made with the Service contract with no major issues outstanding. This activity is on track to work through formal governance and sign off is expected in late August 2020.
- A standing executive meeting now occurs every 6 weeks with Executives from both POL (Nick Read & Jeff Smyth) and Ingenico (Dan Martensson, VP Global Enterprise Sales & Regional Marketing, and Paula Felstead, Global CTO). Ingenico continue to provide commitment to achieve full accreditation by the end of December 2020.

Target Operating Model (TOM) Workstream Update

The focus of the Target Operating Model workstream is to review the Products and Processes that use Card Holder Data and to remediate and remove them from the scope of the PCI DSS audit where possible. If removal is not possible then PCI DSS controls will be put in place. A plan has been prepared to remediate the products and processes.

- The TOM plan has been substantially updated and 7 releases have been identified. A dashboard illustrating the scope, supplier involvement and timelines can be found in the Appendix 2. Key achievements this period are listed below:
- Release A: Obfuscation of PCI data on screens and receipts. The solution for this has been developed and the release has now completed Model Office testing.

Confidential

2

8.1



- Release B: Telephone payments. A solution and contract have been agreed with Verizon. A PO has been raised with Verizon for the PCI PAL solution. Voice recordings to be deleted - speech analytics is no longer required.
- Release D: Travel money card top-up process remediation. A solution design has been proposed to Fujitsu and they are providing an execution quotation.

Commented [JS1]: PCI PAL – don't understand this PAL term

2. What are the key risks on the programme?

The following are identified as key risks:

Risk: There is a risk that any changes needed to the Fujitsu/Ingenico software will impact the plan. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis of no further changes.

Mitigation: Post Office continue to review design documentation and interim software releases to validate requirements traceability. A number of items have been identified and these are currently under review and under impact assessment with the suppliers. Where new requirements are identified an impact assessment will be completed to include any impact to time and cost.

Risk: There is a risk that the software (Mimecast) that alerts and blocks of processing of PCI data cannot be implemented in time.

Mitigation: Post Office team is discussing this with security and IT to find a way forwards and the risk will be qualified in the next reporting period.

Risk: There is a risk that JPM (DXC) & Santander cannot migrate services to route through Vocalink within the timescales.

Mitigation: Post Office team is working closely with DXC/JPM & Santander to produce proposals including costs and timescales. A fall-back contingency solution that requires additional Ingenico development has been tabled but this is likely to cause delays. Planning sessions are underway to examine the options relating to DXC/JPM (which relates to POCA card management) and Santander (to expedite their changes).

Risk: There is a risk that Coronavirus may impact the delivery timescales for any supplier across the entire PCI programme. The outbreak of Coronavirus is a global risk event and the overall impact for the programme is not fully evaluated. Consequently, there may be a delay to the some or all of the agreed deliverables which could affect the build or deployment programme stages. Our risk assessment activity has been expanded to include the potential impact of any remediation work that has a high dependency on Indian offshore resources and in parallel, evaluation of how any second spikes could influence our delivery or implementation timetable.

Mitigation: Post Office is working with all engaged suppliers to better understand their contingency plans to ensure that delivery momentum is maintained. This includes the examination of options to minimise delivery impact by understanding key delivery person risks, supply chain risks and other indirect or latent dependency factors.

8.1

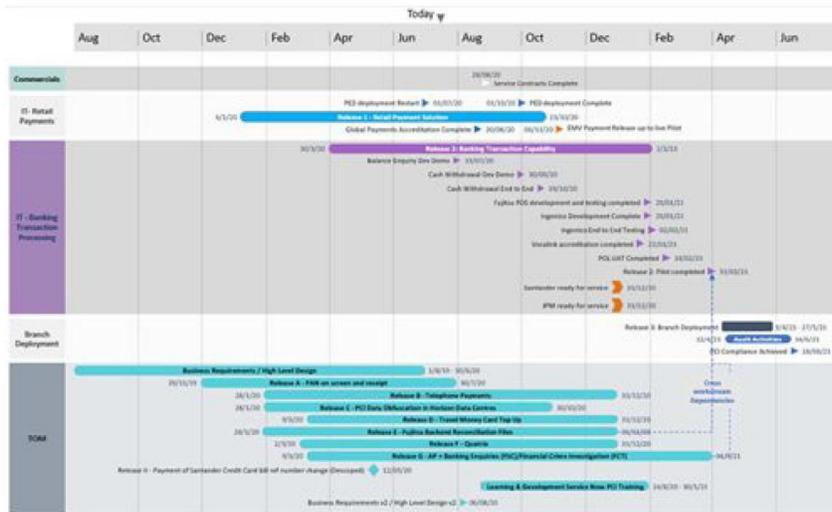
Commented [JS2]: This is another new one for me. I though that Mimecast was an email related system – can we rephrase this so any impact is clearer ?

Confidential

3



Appendix 1 Programme plan



The programme plan has been brought forward 2 weeks since the last report.

8.1

Confidential



Appendix 3 Finance Summary

PCI Programme Capex & Exceptional Spend (2018-2022)	Spend To Date (Incl. Apr-Jun 2020)	2020/21	2020/21	2021/22	LIFE
		[F/Cast] (Apr'20-Mar'21)	[F/Cast] (Jul'20-Mar'21)	[F/Cast]	
		FY	FY	FY	LIFE
Internal Labour	£284,349	£583,145	£441,384	£157,901	£883,635
External Labour	£1,166,655	£579,111	£428,688	£130,875	£1,726,218
3rd Party Costs	£5,488,385	£8,667,274	£6,906,443	£769,443	£13,164,271
Exceptional Costs	£115,000	£0	£0	£0	£115,000
Actual / Forecast	£7,054,389	£9,829,530	£7,776,515	£1,058,219	£15,889,123
3rd Party Costs Comprise					
Fujitsu	£3,476,254	£3,587,244	£4,116,176	£346,536	£8,089,018
Computacenter UK Ltd	£1,382,419	£426,589	£386,885	£7,714	£1,776,817
Atos	£339,010	£652,019	£515,020	£87,508	£941,538
Vocalink	£125,290	£365,740	£277,888	£0	£409,177
Other / TBC	£215,381	£1,635,282	£1,610,674	£127,865	£1,953,922

8.1

Confidential

6



POST OFFICE LIMITED AUDIT & RISK COMMITTEE

Title:	Cyber Security Strategy Update	Meeting Date:	13 July 2020
Author:	Tony Jowett, Chief Information Security Officer	Sponsor:	Jeff Smyth, Interim Group CIO

Input Sought: Noting

- To note the Deloitte Cyber Maturity assessment findings
- To note the impact of COVID-19 on user behaviour and our plans to address this

Previous Governance Oversight

- None.

Executive Summary

The Deloitte Cyber Maturity Assessment shows that good progress has been across the 17 capabilities assessed. A high-level set of actions will be released, and the full report is to follow.

We have been tracking statistics surrounding email-based attacks and user behaviour during the COVID-19 period. The results of this and follow on actions are included.

8.2

Questions addressed

1. What are the results of the Deloitte Cyber Maturity Assessment?
2. What is the impact of COVID-19 on email attacks and user behaviour?



Report – Cyber Security Maturity Assessment

3. In March 2019 Internal Audit and Deloitte performed an assessment of POL's cyber security maturity using their Cyber Security Framework model and toolkit. The assessment measured the maturity of POL against 34 Cyber capabilities and calculated the gap between those scores and an agreed target maturity based on retail and FS benchmarks. Since that assessment, a coherent programme of work has been underway to close the maturity gaps and move POL towards the agreed target maturity values. Progress on this programme has been reported to the RCC and ARC at each meeting since.
4. In April 2020 Deloitte were re-engaged to assist Internal Audit in checking our progress against 17 of the 34 capabilities. The 17 were selected based on risk and importance to POL based on the current business environment.
5. We have internally tracked progress on all capabilities using our own measurement method which has previously been reported at this forum.
6. Deloitte will issue a full report containing detailed actions for POL to further mature Cyber controls later in July 2020.
7. In the interim, Internal Audit have worked with Deloitte to provide an overarching report giving key recommendations and maturity assessments provided. This report is available in the reading room with key results shown in Appendix 1.
8. In summary the results show that:
 - a. We have notable strengths in cyber security and some areas to continue focusing on to achieve target maturity.
 - b. 12 cyber capabilities have increased in maturity, some significantly around data, threat intelligence and SOC/monitoring.
 - c. 3 capabilities have stayed at the same maturity levels since the last review namely cloud security, privileged user access control, and security platform administration.
 - d. 2 capabilities have decreased in maturity, namely strategy & operating model and policies, standards, and architecture.
9. Whilst most areas have increased in maturity the key question is - are we any less secure because of the areas that have stayed the same or reduced?
 - a. Of the 3 capabilities that have stayed the same privileged user access control is already at target maturity. Cloud security has stayed the same as we are mid-way through changing our cloud security strategy to be based more around AWS. Security platform administration has stayed the same as we have genuinely not changed how we are running our platforms. All these three have

8.2

Confidential

2



relatively high maturity scores (e.g. 2.xx) and would not adversely affect our security position.

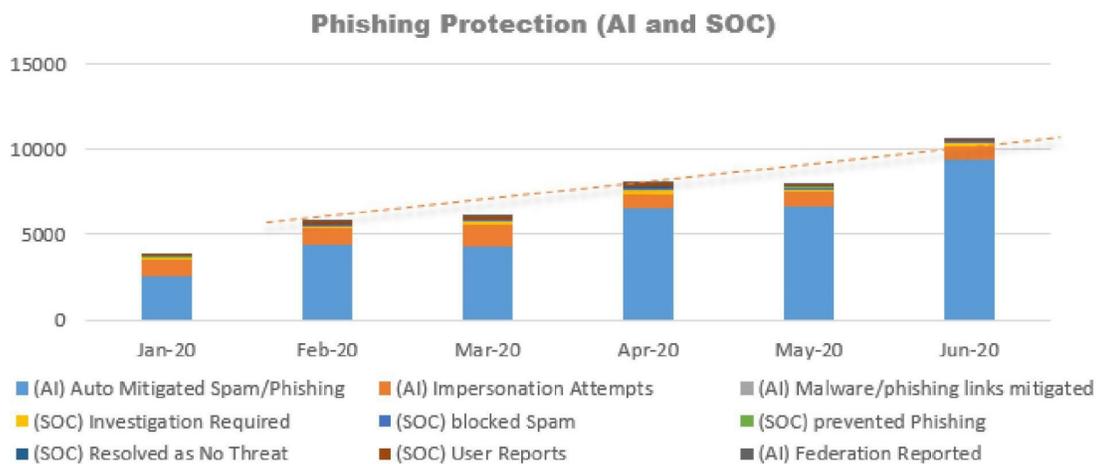
- b. For the 2 that have reduced the rationale is similar. Cyber strategies require an agreed business and corresponding IT strategy to provide context and help define strategic outcomes. As both are currently under development within POL then development of a 3-5-year cyber strategy was not sensible in 2019/20 and this was replaced by tactical rolling one-year plan. Also, Security architecture exists to support the cyber strategy which again explains why the score has reduced slightly in this area.
- c. During the last 12 months we have focused on enhancing the operating model, putting in place a fit for purpose cyber team and CISO. Deloitte have assessed and marked this appropriately.
- d. In answer to the question posed at the start of this section is that we are overall in a more secure place than we were a year ago but in the next year we need to focus on continuing our pursuit of cyber maturity, including the development of a cyber strategy as the business and IT strategies unfold.

8.2



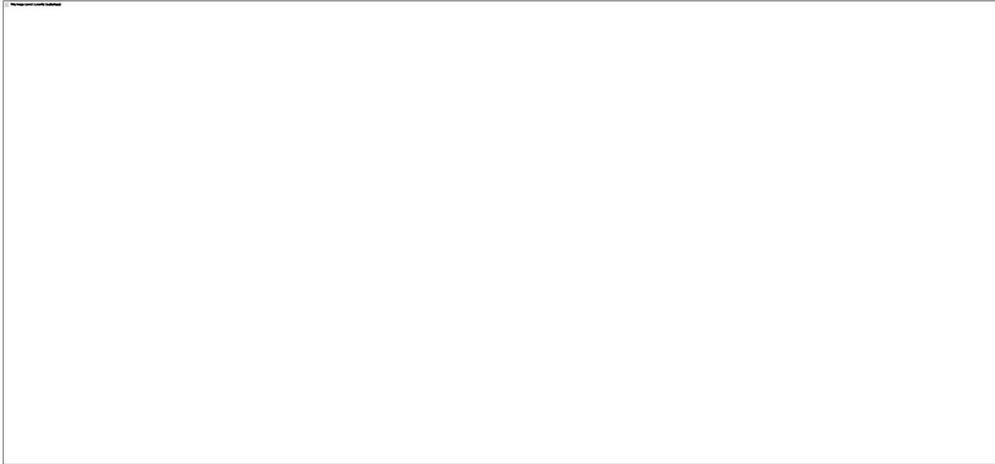
Report - COVID-19 Email & User behaviour

10. In the previous report to this committee we described the steps we have taken to keep POL secure throughout the changes brought about by the COVID-19 pandemic.
11. We have been logging and monitoring some key metrics since January which illustrate the changes during the COVID19 period.
12. The graph below shows the status regarding phishing attacks on Post Office:



8.2

13. Phishing has risen and is continuing to rise as a method of attacking organisations.
14. Our phishing defences continue to work well but we need to stay focused. We have already run a targeted phishing simulation to raise awareness and will be targeting further activity in this area going forward – I am being vague here to keep the element of surprise!
15. The second graph below shows the spike in SPAM-based mail attacks over the COVID-19 initial period which now appear to have returned to normal levels.

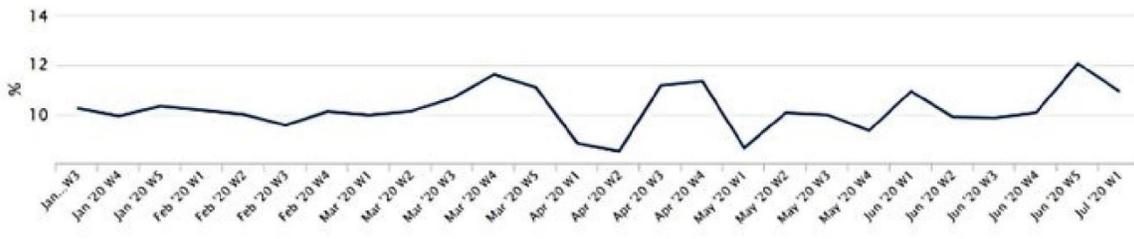


16. Finally, the following graph shows how user behaviour around sending emails to personal addresses with attachments has changed. During March to June, after COVID hit, there was disruption to people’s working patterns and new policies in place regarding home printing. People were developing new ways of working at home which is why we have the large variation in values during this time.
17. Levels have now stabilised. We continue to contact those who break policy in this way to gently remind them of their responsibilities during this challenging time.

8.2

KPI 001 - Personal E-Mail Send w/Attachments User Base Breach % - 6 months

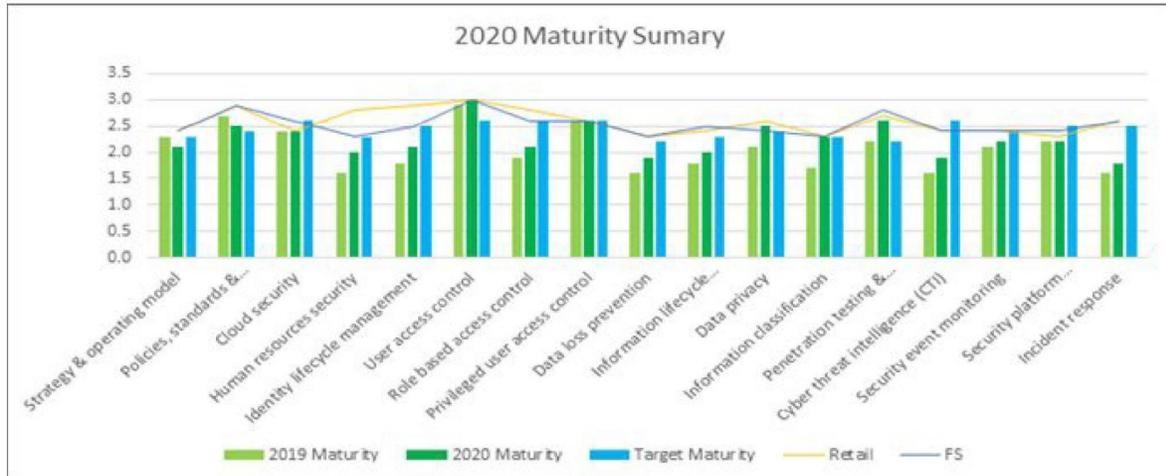
A count of unique users each week who have breached the policy, divided by the total active user population count in that period.



18. The residual percentage is quite high at 12%. This is due to a population of users within POL who need to send emails to personal addresses for business reasons e.g., some of those in branches. Our phase 2 DLP programme will provide the capability to identify these users allowing us to focus on the remainder.



Appendix 1 – Cyber Security Maturity Assessment



8.2

Overarching Actions

A number of overarching actions have been agreed which reflect themes identified during the review and work needed to define target maturity and track actions. Detailed recommendations for each capability will be included in Deloitte’s full report. Internal Audit will track progress against these 8 actions.

Action	Rating*	Action Owner	Date
Scope Area: Governance			
1	P1	Tony Jowett	30 Sep 2020
2	P2	Tony Jowett	30 Sep 2020
3	P1	Tony Jowett	31 Dec 2020
4	P1	Dave King	31 Dec 2020
5	P2	Tony Jowett	31 Mar 2021
6	P1	Tony Hogg	30 Sep 2020
Scope Area: Secure			
7	P2	Tony Jowett	31 Mar 2021
8	P2	Adam Malach	31 Dec 2020

*P1 = High Priority, P2= Medium Priority, P3 = Low Priority



POST OFFICE LIMITED AUDIT & RISK COMMITTEE

Title:	JML Update	Meeting Date:	20 July 2020
Author:	Tony Jowett, Chief Information Security Officer	Sponsor:	Jeff Smyth, Interim Group CIO

Input Sought: Noting

- To note the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML)

Previous Governance Oversight

- Actions to report on this occurred at the previous Risk and Compliance Committee (RCC) in March 2020.

Executive Summary

Joiners, movers, and leavers continues to be a focus area with relevant findings in this area to come from the Deloitte review mentioned above. Key activities and next actions are included.

8.3

Questions addressed

1. What is the status and plans surrounding Joiners, Movers and Leavers?



Report

Tactical Activities

2. We have continued with our tactical activities on JML around:
 - a. Colleague and contractor JML with standard access
 - b. Colleague and contractor JML for privileged access
 - c. Third party access to physical locations
 - d. Third party running JML on their own systems on behalf of POL
 - e. Underpinning technical infrastructure
 - f. Automation and centralisation
3. Our efforts to improve **colleague and contractor JML with standard access** have focused around a project to enhance the integrity of the links between our HR system of reference Success Factors, Microsoft Identity Manager and Active Directory which controls access across the administration estate. This project is in flight and is expected to complete in August 2020.
4. In addition to this work there are several systems that we have anecdotal evidence are not being updated correctly – further investigation is required in Q2 to establish which ones are missing.
5. For **colleague and contractor JML with privileged access** there were 3 recommendations in the PWC financial audit two of which were against Horizon and one against Credence. One of these is closed with an effective control in place. The other two are being investigated further to understand what the next actions are.
6. For **third party access to physical locations** we have paused any activity in this area due to COVID-19.
7. We have examined more closely our arrangements for **Third party running JML on their own systems on behalf of POL**. The Cyber Security team run quarterly Information Security Management Fora to discuss issues and monitor remediations with our main tower vendors. The table in Appendix 1 shows the summary status of the tower vendors regarding JML and Privileged Access Management (PAM).
8. In short, we are currently relying on an attestation alone approach. Best practice is to supplement this with periodic spot audits to keep suppliers honest. Therefore, our next steps are to investigate how we would achieve this under the current contractual arrangements and resourcing.
9. At this stage we do not think it is sensible for us to manage JML on behalf of suppliers under current arrangements. However, the move to cloud (such as that in progress for the Belfast Exit project) presents opportunities for us to have greater oversight and control over JML in the future.

8.3



Responding to the Changing Operating Model & Business Environment

10. Since embarking on the JML programme there have been several significant changes that affect JML:
 - a. The colleague operating model has changed from office-based to being remote with the likelihood of it being hybrid in the future.
 - b. We are adopting a cloud-based strategy for some of our existing tower vendor outsourced systems, the first of these being around Belfast data centre exit. This raises questions about arrangements, ownership and scope of JML.
 - c. New Post Office operating models under SPM and NEO programmes will have an impact the JML.
 - d. The End User Computing (EUC) programme will deliver new and more capable end user devices that can take advantage of modern identity management features such as biometrics and two factor authentication that can further enable hybrid working

11. The collective impact of these on JML is unknown. To resolve these unknowns and to increase JML maturity within POL we are proposing the following strategic programme of work to develop a vision and target operating model for JML for the near future in POL.
 - a. **Confirm the breadth and depth of coverage** of the POL JML regime including answers to how we work with or cover areas that are currently unclear such as:
 - i. Post Office Insurance.
 - ii. Payzone.
 - iii. Tower vendors - depth of control and coverage
 - iv. Cloud – AWS as the first example but there will be others.

 - b. **Establish baseline measures** for JML, to cover but not limited to the following areas:
 - i. Efficiency & cost – to stay affordable
 - ii. Audit & compliance – helping us to meet our internal control standards
 - iii. Security & Risk – helping to reduce insider risk
 - iv. Business enablement – covering our new operating models

This will allow us to target areas of greatest need and to develop business justification for any needed investment.

 - c. **Develop a Strategy Identity Vision & Roadmap** In parallel with above bring in professional help to develop Identity TOM and technology strategy for us. Develop and agree a vision of what done/good looks like (informed by the metrics) and taking into account our new ways of working. Also take into

8.3



account the findings from the Deloitte Maturity Assessment that has been recently concluded. Outputs are:

- i. JML Process Reference model which shows how we have robust controls, process flows and ownership across the scope of the JML regime.
- ii. An identity management organisation model (virtual or physical) to govern and control Identity and JML with clear roles and responsibilities for all involved.
- iii. Recommendations for tools & automation balancing the need for cost control, demonstration of effective controls and risk mitigation.
- iv. Development of a roadmap to deliver the necessary changes.

d. Agree the approach, secure funding, and deliver

12. A roadmap for JML is included in Appendix 2.

8.3

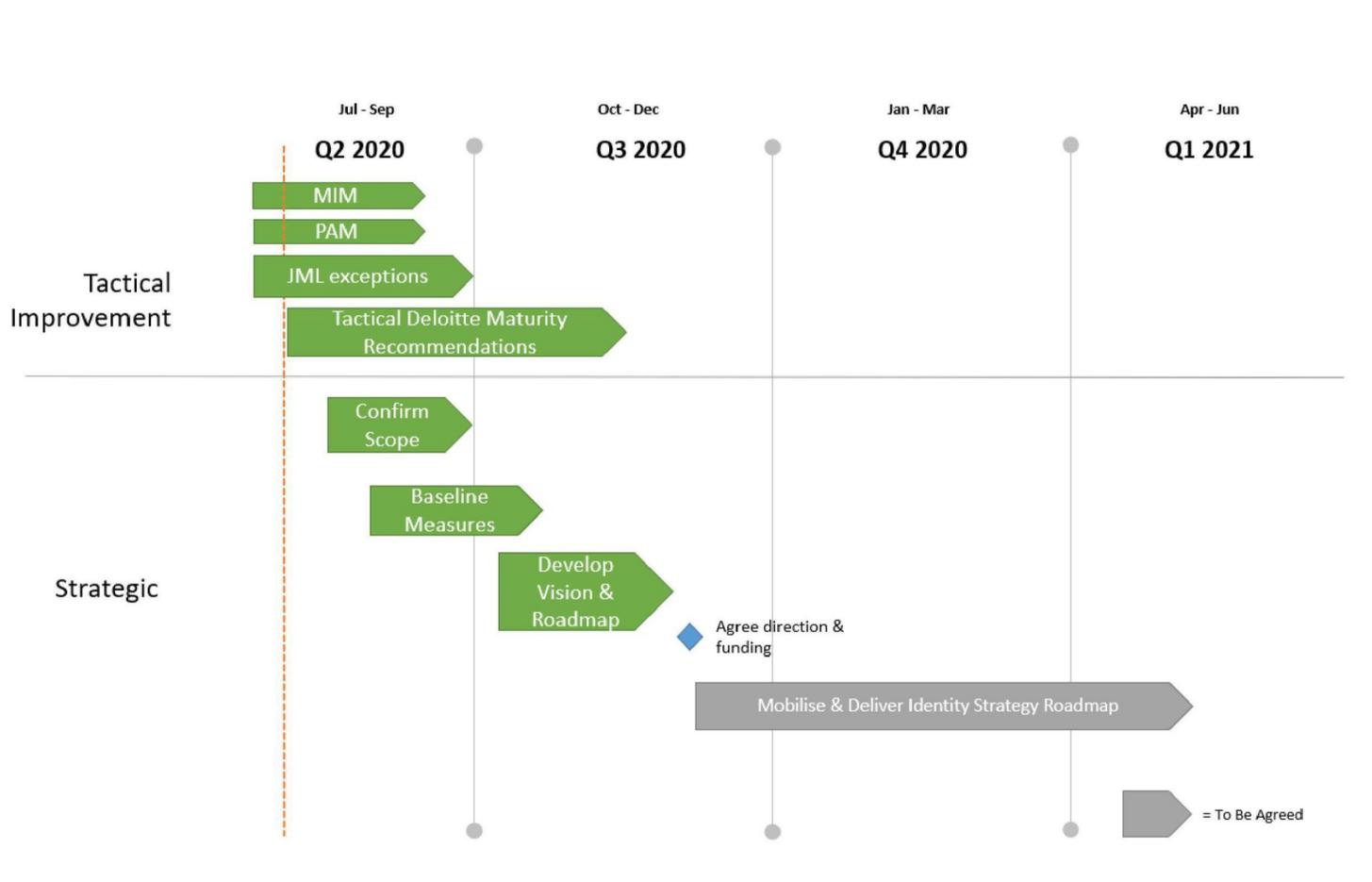


Appendix 1 – Tower vendor JML & PAM status

Vendor	Monthly JML Data	PAM Data
Atos	Provide monthly data on helpdesk staff – Current Staff List and Clearance level.	Not applicable
Accenture	Basic JML Data Provided Monthly, this included clearance and awareness training figures	Quarterly
Computacenter	Basic JML Data Provided Monthly, this included clearance and awareness training figures	Quarterly
Fujitsu Services	Comprehensive list provided monthly.	Monthly
Fujitsu Telecom	Basic data on privileged and user access accounts	As per monthly data.
Verizon	Provide Privileged Management Data on Post Office side. The Verizon staff audits covered separately Verizon staff	Discussed previously at ISMF , this was limited that providing this data provided limited value(it related to Verizon staff not visible to POL) - The JML checks (security clearance an training) are covered by the teams own ISMS and audited several times.

8.3

Appendix 2 – JML Roadmap





POST OFFICE LIMITED RISK & COMPLIANCE COMMITTEE

Title:	Business Continuity and Resilience Update	Meeting Date:	13 July 2020
Author:	Tim Armit, Business Continuity	Sponsor:	Jeff Smyth, Interim Group CIO

Input Sought: Noting and Policy Sign Off

- Report at request of the committee
- Business Continuity Policy requires annual sign off

Executive Summary

Business continuity solutions and levels of resilience have enabled the strong Covid19 response.

Third parties, stakeholders and external organisations have all asked Post Office for business continuity advice across the Covid19 period.

Home working has offered a potential new approach to administration buildings recovery strategy.

Crisis response and communication has been proven to be effective.

Consideration for a Covid19 second wave are now having war games discussed to stress test preparedness.

The business response to a complete Horizon failure remains the key risk.

The Business Continuity Policy requires annual signing.

Questions addressed

1. Do current levels of resilience and continuity plans in place meet Post Office requirements?
2. Are there key business continuity risks the Post Office is exposed to?
3. Annual sign off of the Business Continuity Policy is required



Report

4. Do current levels of resilience and continuity plans in place meet POL requirements?

Yes, the current approach to resilience and continuity ensure that Post Office can respond to major incidents in a timely and controlled manner.

Continuity plans were implemented in February 2020 in preparation for the increased impact of the Covid19 pandemic. When lockdown was implemented home working was in place and solutions to support branches and Supply Chain already implemented.

Physical relocation solutions for Chesterfield, Bristol, Bolton and London are in place with Sungard and these have all been tested and proven to work. However Covid19 has demonstrated that Post Office can run 100% of administration offices with home working for an unlimited period of time. The ability to maintain call centres with home working was successful leading to Post Office being able to support the third party POCA call centre who did not have the same level of response plans in place. Changing to this as an ongoing continuity solution is now being considered and explored.

IT, HR and Communications all had to adapt their plans in place to support the levels of home working required and implement Policy and communications tools to enable and support home working for all administration staff.

Incident response and escalation methods are in place for all levels of incident. A new sub team to respond to branch incidents has been stood up and proven which links into the Business Protection team (BPT). The IT incident response team and its links to the BPT are proven and known by all involved. For specific ongoing longer term crisis events such as GLO post trial response and Covid19 a sub set of the BPT has been stood up and worked as a Rapid Response Team (RRT).

The RRT for Covid19 was stood up in mid-February 2020 to implement the plans and strategies to ensure Post Office continued operations against a number of scenarios. These plans were in place when lockdown was announced and minimised the impact on operations.

Post Office has been recognised by Government and across the Finance system as being ahead of most in their response, planning and ability to smoothly continue operations ensuring that :

- Call centres remained operational
- Circa 9000 branches continued to trade
- POCA services were delivered to all customers
- Working daily with RMG parcel levels exceeded Christmas levels
- Banking services found new personal banking customers as many banks closed
- Supply Chain continued to deliver and return cash and stock as required
- Payzone remained operational across the period
- Specific support was given by individual Post Masters to vulnerable customers

The Post Office on Wheels implemented in December 2019 has been deployed in conjunction with temporary Post Masters and mobile Post Offices to support any branch closures in key areas and ensured if critical branches could not trade a solution could be put in place.

Daily reporting against key metrics, branch closures, employee absenteeism and call centre capability were delivered across the period and developed into operational dashboards.



Grapevine communications support, Sungard third party provider of recovery space and Post Office key IT suppliers all maintained service across the period and have proven recovery capabilities in place.

Post Office has had strong business continuity solutions in place for three years and this exceptional crisis event has again proven the plans in place work, the crisis response is well rehearsed and implemented and that Post Office can be confident it can respond to crisis events in a controlled manner to meet business needs.

5. Are there key continuity risks the Post Office is exposed to?

Yes, there is no coordinated strategy for the large scale failure of the Horizon system; this risk was identified in late 2018 and work was completed across all products and business areas and remains as reported in previous RRC and ARC meetings.

Ongoing work with product teams and IT on alternative solutions continues. The key is to ensure the systems are fully resilient in design with automatic fail over and uninterrupted service. As more services are transferred from the traditional Belfast datacentres to the AWS cloud resilience and reliability will increase and the capability to restore systems during an interruption will be enhanced.

6. Business Continuity Policy requires annual sign off

Policy attached for annual review and sign off.

Stakeholder Implications

7. Resilience and continuity uniquely covers every aspect of infrastructure, operations and leadership as well as external supply chain, as such it liaises and supports stakeholders in all areas.

9

Next Steps & Timelines

8. Ensure lessons learnt from Covid19 enhance planning and are included in future projects to increase ongoing resilience.
9. Support working at home projects, NEO and other developments evolving from Covid19 to ensure resilience is in design.
10. Ensure key areas, GE, HR, Communications are continually trained and rehearsed against scenarios to keep a strong response capability in place.
11. Ensure plans for a second wave or partial lockdowns are in place
12. Focus on Horizon resilience levels and continue to develop alternative working practices.
13. Support IT in reviewing root cause analysis and ensuring operational mitigations continue to meet business needs.
14. Continue to escalate the Post Office on wheels solution.



POST OFFICE LIMITED COMMITTEE REPORT

Title:	Law & Trends Report	Meeting Date:	27 July
Author:	Sarah Gray (Legal Director)	Sponsor:	Ben Foat (General Counsel)

Input Sought:

Noting:

The Board is asked to note the new or proposed material changes to laws and regulations this month.

Previous Governance Oversight

Discussed at RCC 13/07/2020

Executive Summary

There are 3 matters for the Committee to note (details of which are set out in the Appendix):

1. Employment Legislation Update (COVID-19)
2. ATM Additional Business Rates Update
3. Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations

Those matters that relate to Covid-19 are continuously monitored to assess the short and long term risks and potential impact to the Post Office through the relevant working groups that have been stood up and a robust governance framework.

With regard to the other matters referred to, significant work has already been undertaken to ensure any material risks that may arise for the Post Office are being managed to ensure compliance. Where no action is required, the matter has been noted and any further developments will be reported on.

Appendix 1

1. Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
Employment Legislation Update (COVID-19)	<p>Due to the impact of COVID-19, there have been many legislative changes in the employment landscape in order to accommodate and effectively react to the changing requirements.</p> <p>The Coronavirus Act 2020 was introduced by the Government on the 19 March and came into force on the 25 March. The Act introduces emergency powers to handle the COVID-19 pandemic, and out of this introduces several employment changes. There has also been changes made to existing employment legislation.</p>	<p>In the May RCC Law & Trends report, updates were provided on the following legislation:</p> <p>a) <u>Coronavirus Job Retention Scheme</u> ('JR Scheme')</p> <p>b) <u>Emergency Volunteering Scheme</u> ('EV Scheme') -</p> <p>c) <u>Working Time (Coronavirus) (Amendment) Regulations 2020 - Carry-over of Annual Leave</u></p> <p>This regulation was brought in very quickly and the expected subsequent guidance and legislation failed to appear. With the easing of lockdown it appears unlikely that this will ever materialise and focus is on how Post Office can support the easing of lockdown for those that wish to return to work.</p>	<p>Although work was undertaken to explore whether Post Office would want to take advantage of the JR Scheme, the decision was made not to furlough anyone and in any case the JR scheme has closed to applicants now.</p> <p>The focus for Post Office is on supporting people returning to work through the exceptional circumstance policy and ensuring the workplace is compliant with all the COVID-19 related guidance. As it stands, HR have received 10 requests from employees regarding returning to work.</p> <p>Risk assessments are taking place and the Health & Safety Team are heavily involved in working through the results of these.</p>	<p>The relevant working groups continue to work through government guidance as and when it is being published to ensure Post Office is compliant.</p> <p>Post Office policies and guidance are being updated regularly and disseminated throughout the business as appropriate.</p>	RAG
<p>ATM Additional Business Rates Update</p> <p>Appeal of Cardtronics UK Limited and others v Sykes and others</p>	<p>The appeal concerned the treatment of ATMs for business rating purposes situated in supermarkets or shops owned and operated by the retailers. The Valuation Office Agency ('VOA') changed its practice in 2010 and started to assess ATMs separately for additional business rates where they did not form a part of a bank branch.</p> <p>There were two main issues:</p>	<p>In 2014, due to the unique contractual arrangement of Post Office and Bank of Ireland, Post Office received a confirmation letter from the VOA that they would exercise its operational right to not separately assess Post Office ATMs and therefore Post Office didn't have to pay additional rates on separately assessed ATMs.</p> <p>However, in 2018 the VOA changed their appeals system meaning that Post Office could no longer rely on this letter and therefore since 2018 has been incurring</p>	<p>Now that the Supreme Court has made final judgment and no further appeals can be made, the effect of that decision means that Post Office can move forward in escalating and challenging the ATMS that were assessed separately and claiming a rebate.</p> <p>There are approximately 53 ATMs that Post Office have been paying ATM rates on that total £354k; we are unable to claim for the backdated charges from 2014-2017 meaning Post Office are only entitled to claim back £297k. The backdated charges</p>	<p>Post Office has already engaged with Bank of Ireland, however is also going to engage with the VOA to ascertain whether there is a one-off exercise that can be undertaken centrally due to the unique contractual relationship with Post Office and Bank of Ireland in relation to ATMs to address the rebate.</p> <p>Rates are usually paid pending a challenge and the Rates Bill for 2020/2021 for England & Wales ATMs would total £109,000. Post Office is also going to enquire as to whether these rates can be put on hold to avoid</p>	RAG



Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	<p>1) Whether the sites of the ATMs are to be properly identified as separate hereditaments from the stores</p> <p>2) Who was in rateable occupation of the separate hereditaments and therefore responsible for the additional business rates</p>	<p>charges on around 53 ATMs totalling £354k.</p> <p>Due to the ongoing case, Post Office was advised to wait for the outcome before escalating this situation.</p>	<p>were in a different valuation roll and therefore had to be challenged by 31 March 2018, following advice to wait for the outcome of the case to challenge, we are now unable to claim back for this amount.</p> <p>Rebates are completed via the on-line system, but only the occupier for the site of the ATM can register for an account in order to make these challenges; legally Bank of Ireland are the occupier and therefore will need to register themselves, although it is Post Office who will be entitled to the refund as it is Post Office who have incurred the cost.</p>	<p>paying this payment and then having to claim a rebate in quick succession.</p>	
<p>Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations (the 'Regulations')</p>	<p>The Regulations introduce obligations for Public Bodies to make websites and mobile applications accessible for people with disabilities.</p> <p>Complying with accessibility standards has always been best practice for designers and developers however due to various factors it became hard to oversee and compliance with the standards dropped. The Government has now introduced the standards as law which has effectively forced the hand of public sector bodies to comply.</p>	<p>Accompanying government guidance to the regulations states websites and mobile applications will comply if they meet the WCAG2.1AA Accessibility Standards.</p> <p>The standards identify issues and set standards for ensuring websites and applications can be used by disabled people, taking into account both their disability and the equipment or software they may use as an aid. Some examples are:</p> <ul style="list-style-type: none"> - Ensuring a website can be navigated using a keyboard rather than a mouse; - Avoiding use of certain problematic add-ins; - Making sure image size and quality is appropriate; and - Ensuring adequate colour contrast to make text and images legible to the visually impaired. <p>A public body does not have to comply where compliance would impose a 'disproportionate burden'. To determine a disproportionate burden, the public body must consider its own size and resources, the cost and difficulty of the remediating measures and the benefits which implementing these remediating measures would provide for a disabled user.</p>	<p>The Regulations apply to Post Office as a 'body governed by public law'.</p> <p>Obligations for accessibility will apply to Post Office's websites from 23 September 2020 and to its mobile applications from 23 June 2021. Although some organisations are contractually obliged to meet these standards or self-accredit, formal compliance with the standards is new for Post Office.</p> <p>Post Office has done the following in order to address the introduction of the Regulations:</p> <ul style="list-style-type: none"> - A period of insourcing talent to ensure consistency across digital design and development and greater oversight; - Changing the procurement process so the on-boarding includes references to compliance to web standards and accessibility; and - Bringing in AbilityNet to carry out a third party audit to assess the extent of the accessibility issues. <p>The results of the audit showed that across the core touch points of the Post Office websites and high level across the whole</p>	<p>The Digital Innovation Team's view is that come September, Post Office will be in a good position with respect to compliance with the Regulations.</p> <p>Further work will continue to engage with sub-contractors and stakeholders as appropriate.</p> <p>The Digital Innovation team is also looking to engage several charities such as Mind, to complete testing on the new designs.</p> <p>Mobile applications have to be compliant by 23 June 2021, and although the priority is the website, budget has been allocated for an audit by AbilityNet on the Post Office mobile applications.</p>	



Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		<p>The public body must also produce an Accessibility Statement. This must include details of which parts of the website are not accessible and why, as well as contact details so a user can both notify the body of any failures to comply with the Regulations and request a copy of any information a disabled user cannot obtain as a result of such failures.</p>	<p>site there were 1000 accessibility issues. In order to address all issues the core platform of the Post Office website would have to be created from scratch and therefore Post Office’s approach is to address all the accessibility issues that it possibly can. The Digital Innovation team is working closely with Legal and Compliance in order to get to a position where there is comfort that Post Office has remediated everything it can and be confident in the Accessibility Statement that it produces.</p> <p>It has also been identified that Post Office doesn’t own the code for all its digital platforms Corporate Website etc.) which leaves Post Office with no ability to address accessibility issues. The Digital Innovation team is engaged with Legal and Compliance in order to address how we can engage those stakeholders in relation to the Regulations.</p>		



POST OFFICE LIMITED AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Risk, Compliance and Audit Report	Meeting Date:	27 July 2020
Author:	Mark Baldock: Head of Risk Jonathan Hill: Director, Compliance Johann Appel: Head of Internal Audit	Sponsor:	Al Cameron: Chief Financial Officer Ben Foat: General Counsel

Input Sought: Noting

Previous Governance Oversight: Not applicable

Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position. The Committee is asked to:

1. Note the Risk update, specifically:
 - the status of the Post Office's risk data set and the key risks
 - the Post Office's approach to risk appetite and Key Risk Indicators
 - how the Post Office is embedding accountability and responsibility for the management of its risks
 - the new Risk Lead role
 - the status of the Change Portfolio and key delivery challenges.
2. Note the Compliance update, in particular the review of accountabilities, controls and culture.
3. Note the Internal Audit update, specifically:
 - analysis of internal control themes from 2019/20
 - audit report clearance metrics
 - progress being made with delivery of the Internal Audit programme and completion of audit actions
 - that the Deloitte co-source agreement will expire on 30 September 2020 and we intend to extend the agreement for a further two years, whereafter the service will be subject to a re-tender process.



Risk

Questions addressed

1. What is the status of the Post Office's risk data set and what are the key risks?
2. What is the Post Office's approach to risk appetite and Key Risk Indicators?
3. How is the Post Office embedding accountability and responsibility for the management of its risks?
4. What is the new Risk Lead role?
5. What is the status of the Change Portfolio and key delivery challenges?

The Post Office's risk data set & the key risks

- 1 In 2/2020 we (in Central Risk) facilitated a discussion with GE to discuss the key business risks faced by the Post Office and their (then) current RAG status and relative priority. Following that discussion we have now completed work on the articulation of a new Post Office-wide three-tiered risk data set comprising (i) **15** overarching enterprise risks, (ii) **70** linked intermediate risks and (iii) **350** subsidiary local risks. All **435** of these have been uploaded onto RSA Archer (our corporate Governance, Risk and Compliance tool) and arrangements are underway for these risks to now be proactively managed by the business. This work is ongoing but includes **ensuring the business clearly articulate each risk**, (in terms of its cause, the risk itself and its impact), **'grouping' low level risks** to their relevant intermediate and enterprise risks (to give an aggregate risk profile), **assessing risk impact and likelihood consistently** (against corporate standards) and, finally, **outlining clear remediation plans** (with owners and dates).
- 2 At this point the key enterprise risks remain:
 - **Commercial**: Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market
 - **COVID-19**: Risk that the Post Office business employees/postmasters are adversely impacted by the spread of COVID-19 and wider associated socio-economic activity.
 - **Financial**: Risk that the Post Office has insufficient funding and/or uncontrolled costs in the short-, medium and long-term such it is unable to deliver its strategic objectives. This could have a long term impact on commercial viability
 - **Legal**: Risk that the Post Office is unable to comply with legislative and regulatory changes, sectoral regulator guidance and/or the outcome of other external legal activity (i.e. litigation, including GLO) resulting in significant fines, loss in revenue, reputational damage and customer detriment
 - **Technology**: Because the Post Office is heavily reliant on key 3rd IT parties (with limited ability to influence the relationship), has an ageing IT infrastructure, hardware and software there is a risk that it is unable to deliver a new Front Office system and has an ineffective Disaster Recovery regime. If the risk is not proactively treated and materialises this could lead to significant impact to operations and significant reputational damage.
 - **Operational**: Because of low-quality Branch Network locations, unprofitable Retail Partner(s), an unattractive Agency remuneration package and/or badly designed operational core processes & control environment there is a risk that the Post Office operation is not fit for purpose.
- 3 Key intermediate risks include:
 - **Government Services**: The Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) may reduce over the short-, medium-



- and long-term. Work is underway to review a faster roll out of Tablet services to ensure we are ready for the travel bounce-back. Marketing discussions underway for a PO services awareness campaign. Regular liaison with Government Departments to emphasise role PO can play.
- **Digital Income:** Post Office on-line products and services may generate a reduced income level compared to comparable physical products and services. Commercial work underway to determine post-COVID-19 strategy and identify critical markets for Post Office along with the requisite operational functions and dependencies to support them.
- 4 Since the last ARC we have fully assimilated the Post Office COVID-19 risk identification and management activity into our wider enterprise risk work given ongoing separation would have been simply artificial.
- 5 Appendix 1 provides a series of Dashboards (at enterprise, intermediate and risk register level). The data is taken directly from RSA Archer.

Risk Appetite & Key Risk Indicators

- 6 Each risk within the Post Office risk data set is assessed for impact and likelihood against the corporate scoring metric (the Post Office HARM table approved by ARC in 9/2020). This assessment provides each risk with (i) an **inherent score** (before any mitigation is undertaken), (ii) a **residual score** (reflecting the impact of mitigations to date) and a **target score** (an aspirational end point when the business consider the risk can be simply tolerated).
- 7 However for these assessments to be of any value we must be able to differentiate between individual risks with identical impact and likelihood scores. Without this the assessments will simply be too 'crude'. To do this we need different tolerances at a corporate level for different types of risk. We also need a simple early warning system to show us where such tolerability is under strain.
- 8 Given this we have secured GE approval to our proposal to refresh our corporate risk appetite statements (last updated in 2015) and put in place a supporting set of Key Risk Indicators (KRIs). Such approval was on the basis that we
- minimise the bureaucracy and burden on the business and use existing performance data to help shape the associated KRIs;
 - ensure the risk appetite statements cover cross-organisational risks, not just those in organisational silos; and,
 - pilot the approach in 3 areas (i) **Operational/Legal** (ensuring we cover Postmasters/GLO etc), (ii) **IT** (ensuring we cover Technology, Security and extended IT supply chain risks) and (iii) **Finance**.
- 9 We have already begun work on the Operational/Legal and IT risk appetites. This involves
- a) an initial desk-based review by Central Risk and the completion of a simple questionnaire on the topic by key individuals within the business to identify initial options
 - b) a Central Risk-facilitated discussion with the GE members and their senior management team to re-confirm the key risks they face, their associated KPIs and what should be the likely tolerances and acceptable trade-offs to allow them to remain within an agreed level of appetite



- c) the completion by Central Risk and the GE Risk Lead of the final draft Risk Appetite Statement and KRIs for GE sign-off and then submission to RCC/ARC.
- 10 We intend to seek RCC/ARC approval to the final draft outputs from 9/2020. At approval we will produce supporting communications and guidance for the business on how agreed Risk Appetite Statements and KRIs will be governed and can be used pragmatically and sensibly going forwards. We plan for approved risk appetite statements to be subject to yearly review thereafter.

Accountability and Responsibility for management of risk

- 11 Since the last ARC we have also clarified where accountability and responsibility should lie in the business for managing and owning our risks. The GE has re-confirmed its commitment to the industry standard "three lines of defence" risk management model. It is a simple and effective way to delegate and coordinate risk management roles and responsibilities. We have clearly communicated that for the Post Office this means:
- 1st line of defence: The GE Groups (and their individual directorates/units) are the Post Office's 1st line. They own and are accountable for identifying, assessing managing and reporting on their risks. They are also responsible for putting in place internal controls on a day to day basis, ensuring compliance with risk policy and implementing corrective actions to address any deficiencies.
 - 2nd line of defence: We, in Central Risk are the Post Office's 2nd Line with regard to risk (there are other 2nd line functions such as Compliance, Data Protection, Legal etc with other specific areas of focus). We define and implement the Post Office's risk standards, policies, procedures and guidance. We also proactively support and guide the GE Groups in the management of their risks in line with good practice. We alert senior management to emerging issues and changing risk scenarios. We also monitor and report on levels of compliance (including agreeing exceptions to approved risk policies). We report to the GE, RCC and ARC.
 - 3rd line of defence: Internal Audit remain the Post Office's 3rd line. They provide an objective and independent evaluation of how effectively the Post Office assesses and manages our risks, including the operation of the 1st and 2nd lines.

Risk Leads

- 12 To ensure this model works effectively the GE have nominated Risk Leads to proactively coordinate and support the risk work within their respective GE Groups.
- 13 The Risk Lead is an important role. As such the individuals appointed have the requisite authority to help and direct their respective individual directorates/units in identifying, assessing and managing their risks. They will act as role models for Post Office risk management in their GE Group.
- 14 We, in Central Risk, are proactively supporting them in this role through informal training, guidance etc as well as facilitating risk workshops etc. We will also soon be arranging for them (and individual risk owners) to be given direct access to the RSA Archer risk management software tool. This will allow them to access and manage their risks efficiently and effectively on-line and in real-time.

The status of the Change Portfolio, including top risks and key delivery challenges

- 15 By the end of 5/2020 the overall status of the Portfolio remains at Amber. The detailed review of the Change Portfolio, as a result of changing costs and COVID-19 has



continued with a baseline position and options for prioritisation discussed at the Board in May. Prioritisation will continue while under extreme conditions.

- 16 YTD spend by the end of 5/2020 was £6.5m. This was lower than expected due to delays in approvals for litigation spend. YTD benefits achieved were £5.2m which was £1.2m below forecast, driven mainly by product related variances
- 17 Delivery remains amber with a lot of activity around project closures, 4 projects closed in 5/2020 and 9 are planned close by the end of 8/2020. People and Culture programmes are due to commence in the future months.
- 18 The number of gold and platinum projects reporting¹ an overall Red RAG status is **4**. This is unchanged since the last RCC/ARC but the individual projects are different:
 - IDS Digital Identity: In 4/2020 the Portfolio Review Board approved for the IDS In Branch Verification workstream to be de-scoped from this project and established in its own right. This allows the IDS Digital Identity project to proceed to early closure.
 - Paystation Refresh: Rollout has been constrained by (i) Branch availability during lockdown, (ii) stock availability (units are produced in China) and (iii) Ingenico site engineer resource capacity given a number of their sub-contractors have been furloughed. By the end of 6/2020 1300 units (from a total of 3200) had been refreshed. Discussions are underway with BG to adjust the contractual requirement for additional transactional data from 1 August 2020 to 30 September 2020. Informal soundings suggest British Gas are supportive of this given the extenuating circumstances.
 - General Data Protection Regulation (GDPR): Initially Red now Amber because there are a small (but reducing) number of contracts in which the counterparties are not engaging. Plan to continue remediation in BAU.
 - Post GLO (Legal): Level of risk is unquantifiable due to the potential for a high number of referrals to the Court of Appeal which could lead to a high number of overturned convictions
- 19 Appendix 2 provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

11

Compliance

Accountabilities, controls and culture

- 20 Compliance is refreshing the accountabilities matrix for the key legislation and regulations that Post Office is subject to. This was last conducted in 2017.
- 21 Further, as part of the on-going development of compliance in Post Office and, in part, as a result of the challenges raised by the GLO, the Compliance Team, in conjunction with the Change Team, will be conducting a review of the controls in Post Office.
- 22 This review will look at the controls needed to ensure we are meeting our Legislative, Regulatory, Policy and Contractual obligations, their effectiveness and how we can provide on-going assurance. We will also look at opportunities to simplify and synthesise the controls, aiming to reduce omissions and errors.

¹ Post Office Strategic Portfolio Office UKGI report (P2) – May 2020



- 23 It is anticipated that we will work with an external firm to support this work and an RFP will be issued shortly.
- 24 This is a significant programme and therefore we are prioritising the review of IT, Operations, Supply Chain and Mails initially.
- 25 We aim to provide an initial interim report in November 2020.

Telecoms

Responses to Ofcom information requests

- 26 In the March paper we noted that we have identified a number of inaccuracies in previous responses to Ofcom's formal S136 and S137 information requests for Comparing Service Quality. Ofcom were made aware of this issue when it was discovered. Failing to provide accurate and timely responses to requests can result in an investigation by Ofcom's enforcement team and could result in fines.
- 27 Although we are currently planning our exit from the Fujitsu platform, we continue to hold Fujitsu to account of providing a fully compliant service as one of their key contractual responsibilities. The Telecoms team has senior level engagement with Fujitsu to ensure it remains fully committed. The Fujitsu service is already subject to extensive independent audit (e.g., TMBS for customer billing) which has been positive, giving Post Office confidence in the Fujitsu systems and processes for customer billing. We also have several checks in place to ensure customer experience is both positive and compliant. These include spot checks through call listening and reviewing the way agents are assessed for compliance. The Telecoms Compliance Committee also monitors performance on key compliance metrics and the progress of implementation of new regulations. However, the Telecoms Team has acknowledged that recent issues have shown a continued focus on this is required.
- 28 Fujitsu have again been reminded of their contractual responsibility to provide a fully compliant service, using the recent examples of failings and to improve our confidence in the accuracy of the data from Fujitsu in the future, we will be implementing refinements to the process for data that is then provided to Ofcom to include:
 - Approval by a senior level individual in Fujitsu
 - Details of the data validation process to be provided to Post Office i.e. Fujitsu will document the checks they have performed internally to ensure that these have been performed and are adequate
- 29 This may add additional time in for us to respond to Ofcom's requests however it is important that the data is correct and we will make this clear to the regulator at the time of their request to manage their expectations.

Telecoms Providers' response to Coronavirus

- 30 The call centre is stable and has resumed normal activities, with 85% of agents homeworking as of 14th July. Post Office is continuing to prioritise fault repairs for vulnerable customers and honour the commitments made to DCMS. Ofcom are requesting fortnightly updates and have now resumed their monitoring and enforcement programme.

Fairness

- 31 Fairness for customers is an Ofcom priority and it has a significant work plan to help achieve this. Post Office along with all the other major providers signed up to Ofcom's fairness commitments earlier this year which are to ensure:
 - Customers get a fair deal, which is right for their needs.



- Customers get the support they need when their circumstances make them vulnerable.
 - Customers are supported to make well-informed decisions with clear information about their options before, during, and at the end of their contract.
 - Customers' services work as promised, reliably over time.
 - Customers can sign up to, change and leave their services quickly and smoothly.
 - Customers can be confident that fair treatment is a central part of their provider's culture.
- 32 Ofcom will be collecting data over the next few months with a view to publish a report on the fairness commitments in early 2021. At our last meeting with Ofcom they said that they consider customers as "vulnerable" when they have been out of contract for a long time e.g. 2-3 years. Ofcom thought Post Office would be near the top of providers with a high percentage of out of contract customers (paying higher prices than in contract customers). Ofcom said they would 'like progress' on long term out of contract customers. Some providers had already taken steps to address this, e.g.
- BT has provided a one-off automatic price reduction for vulnerable customers who are already out-of-contract.
 - TalkTalk has agreed to carry out an annual review to ensure that its vulnerable customers who are out-of-contract are placed on the best tariff
 - Virgin Media is calling vulnerable customers (including anyone over 65) to get them onto the best contract and, if they do not answer, will automatically move them onto the best available price.
- 33 Budget constraints currently inhibit Post Office from acting in a similar fashion to other providers. It should be noted though that POL have implemented the End of Contract Notification Regulation which is driving customers to contact POL to renew their offer and is achieving good response rates.

Annual Best Tariff Notifications

- 34 Following on from the introduction of End of Contract Notifications, Post Office is required to send Annual Best Tariff Notifications (ABT) to customers who have been out of contract for more than a year and not received an End of Contract Notification. The ABT must be sent by 14th February 2021. The Telecoms Team is aiming to do a trial to assess the impact ABT will have on the call centre so that we can resource effectively. Following on from this the Telecoms Team hope to do a phased approach starting with vulnerable customers.
- 35 This is subject to internal funding sign off. Final costings for delivery across this and other projects by Fujitsu is coming in higher than budget, which is causing the Telecoms Team to have to review its plans to complete the programme in line with the £1.2m initially approved budget.

PSD2

- 36 In January 2020 Post Office wrote to the FCA to inform it of our intention to seek an Electronic Communications Exemption ("ECE"). This requires Post Office to cap premium rate calls at £40 per call and £240 per month in aggregate. We informed the FCA that we would repay any over charged customers going back to when the obligations came into effect on 13th January 2018. The FCA confirmed it was happy with our approach. We wrote back to the FCA on 10th June 2020 to update it on the work we have been doing.
- 37 The FCA responded on 29th June 2020 to thank us for our clear letter and confirm it is happy with the approach we set out. Our next steps will be to:



- submit a first ECE Notification as soon as practicable (the FCA has not given us a hard and fast deadline as it says that most of the works appears to have been done already)
- submit an audit opinion in 2021 (date to be determined)

Emergency Database Update

- 38 Telecoms providers have an obligation to provide the address of a customer to the emergency services when a customer calls them. BT holds an emergency address database and it is common in the industry for mismatches to occur between a provider's address and the address stored in the system for billing purposes. This is because for example, a house gets made into flats, or a postcode gets changed.
- 39 In order to mitigate this, Talk Talk has a process in place to check the addresses on file against the emergency database. When it identifies mismatches it is usually able to correct these. However, in March 2019 Talk Talk informed Fujitsu, who in turn informed Post Office, that there were 568 cases it was unable to reconcile. Post Office began the process of resolving the mismatch and 79% of customers have confirmed their addresses. In the majority of cases it was the emergency database that was incorrect. Of the remaining customers, these have received a letter and received at least 3 outbound calls (both to landline and mobile where applicable) but have not responded so have now had their services limited in order to force them to contact Post Office and confirm their address.
- 40 Currently 99.9% of the addresses on the Post Office system match the emergency database. A new process has been set up so that every month Talk Talk provide any mismatches they cannot resolve and Post Office handle these through a BAU process.

European Electronic Communications Code

- 41 The new European Electronic Communications Code (EECC) will impose new regulatory obligations on all providers. These obligations will include changes to the switching process, additional information about contracts, provision of pre-contract information and accessibility obligations.
- 42 Ofcom recognise that given the very challenging circumstances we are currently in as a result of the coronavirus crisis, providers need additional time to make the necessary changes. Ofcom have said they are now giving providers at least 12 months from the date of the publication of their statement to implement these new rules, with the statement expected to be published in September however these rules were initially due to be implemented by December 2020.
- 43 Given the magnitude of the changes, Compliance and the Telecoms Team are commencing work now to understand how long the changes will take and the costs involved.

Data Protection

GLO and Historic Shortfall Scheme

- 44 Compliance has been working with the GLO project to identify, locate and provide all data required to support the various ongoing initiatives, in particular;
- Working with the Historic Shortfall Scheme to manage and answer all requests for information and data to support applications. As of 17th July 2020 there are currently 73 live requests.
 - There are another c.130 applications that will require additional data to support but we have yet to have requests made to us. These applications gaps range from information about any shortfalls suffered during their tenure through to full complex



- Data Subject Access Requests that could take up to 3 months to complete. We are proposing to the HSS team that Post Office should contact these applicants offering assistance.
- Provide information to support those cases that have been referred by the CCRC. These searches are complex and Compliance is working with external law firms to identify, locate and extrapolate all information that may be required by the Court.
- 45 Given the scale and complexity of these searches, the historic nature of the information and the widespread location of the data this has stretched BAU resources. The GLO SteerCo has approved additional resource to support this work.
- 46 In addition to this direct work, the Data Protection team is dealing with a significant rise in complex Freedom of Information Requests, relating to GLO matters. These requests invariably require external legal support due to their sensitivity and complexity. All requests prior to any disclosure require approval from the GLO SteerCo and notification to UKGI.

GDPR Contract Remediation:

- 47 Please see separate agenda item.

Belfast Data Centre Exit and move to the Cloud

- 48 IT Strategy is to exit the Belfast Data Centre in 2021 and move Horizon to a cloud based solution. Due to the size, scale and complexity of this move an aggressive timescale has been set. To meet these timescales the copying of data from the Belfast Data Centre is planned for eight weeks' time.
- 49 Fundamental to the transition is the management of the risk to the integrity of Horizon data and the implication for Post Office upstream clients such as Government, Banking Services and Bill Payments contracts.
- 50 It was previously reported that the process of moving Post Office data into a cloud environment with access being granted from outside of the EEA would be challenging. IT, in conjunction with AWS, are deploying a solution where all Post Office data will be encrypted in the cloud with Post Office holding the encryption keys.
- 51 This means that even if an incidental transfer were to occur that AWS could not access any of the raw data without Post Office releasing the encryption code. This will be an easier sell to our upstream clients who may be nervous about moving into a cloud based solution.
- 52 IT, Legal and Compliance are working together to deploy a contractual and operational solution that will eradicate the need to consistently seek the approval of upstream clients when personal data may be processed outside of the EEA. Working with external lawyers a compliant solution inside Post Office Risk Appetite has been identified and is currently being developed.
- 53 This new solution will require the notification and/or approval of all upstream clients, which will be challenging given the aggressive timescales of the migration. However, all involved believe this challenge will bring both operational and financial benefits to Post Office and help deliver the CIO's IT Strategy.

Post Office use of Cookies on Internet and Apps

- 54 The solution for resolving the outstanding Cookies issue has been built and been deployed on the Post Office website.
- 55 As previously reported to and agreed by the Committee, this solution does not completely address the new consents guidance from the ICO but it does provide strong protection for customers and helping sustain commercial viability. This does position Post Office "in the pack".



- 56 A recent court case in Germany has ruled that a solution similar to that deployed by Post Office is in breach of German legislation. Whilst this ruling is not directly applicable in the UK, the decision of the CJEU will be taken into account in the interpretation of what constitutes valid consent under UK law. This does not alter Post Office position as being 'middle of the pack' and therefore Compliance are recommending no changes at this point in time.

Financial Crime

Compliance with Money Laundering Regulations

- 57 137 new Bureau de Change cases were identified between 20th April and 19th June 2020 (up 92.9% from the same period in 2019). Most related to low value linked transactions which were deemed suspicious, but there has been a recent increase in higher value Bureau de Change Sell transactions, in line with changes in lockdown rules and international travel.
- 58 The monitoring report introduced in January to identify branches processing multiple transactions just below the threshold for ID has helped us to take action in 5 branches where transactions have been deliberately split.
- 59 The solution to extract the correct data for Sanction Screening has been implemented. Due to the downturn in transactions, no sanction hits have occurred, and until there has been a partial/exact match, the solution cannot be effectively live tested. The manual workaround is still in place and has been effective to date.
- 60 Suspicious Activity Reports and investigations have reached record levels during the lockdown period, with 930 SARs and 159 investigations in April & May (compared to 598 and 84 in April & May 2019).

Anti-Bribery and Corruption ("ABC") update

- 61 The new reporting and approval portal is live, however, some IT issues have been identified, and some modifications are being developed by IT to resolve. There has been minimal reporting during Covid lockdown.

Whistleblowing Update

- 62 The migration to the new Navex Global Ltd platform was completed in May, and further communications and awareness are planned during the summer.
- 63 There has been a slight decrease in new reports in Q1 2020/21, with 8 reports received in comparison to 9 in Q1 2019/20. There continue to be a number of reports against employees at non-customer facing sites (please refer to the Whistleblowing MI in the Reading Room).
- 64 Two branch related investigations remain on hold as a result of Covid-19 restrictions which is making it difficult to undertake visits, but with the ease in lockdown, these will now be progressed.

Fit & Proper update

- 65 The agent F&P data was sent to HMRC on 19th June, following an agreed 2 month suspension. 7 data gaps were identified relating to 6 branches that have been in short term temporary closure status for over a year, and these are being investigated.
- 66 This was the last manual data collation and followed the de-registration of c.6,000 branches that were commercially unviable for Travel Money, or have been temporarily paused as no transactions are currently being undertaken, in order to reduce the cost of annual registration from over £3m to c.£1.3m. HMRC have also deferred payment of the fee from 1st June 2020 until 1st December 2020.



- 67 There have been two meetings with HMRC to discuss fees. The first was to try and identify a solution that prevented the deregistration of the 'paused' branches, but constraints within HMRC systems and policy meant that a mutually satisfactory solution could not be identified, hence the branches will need to be re-registered if and when the Travel Money business picks up.
- 68 The second meeting was for HMRC to discuss with Post Office the forthcoming fees consultation, and understand impacts due to the size of our Network. HMRC shared with Post Office the options they had considered and provided explanation as to why a number were unviable. The three remaining options are based around per premises fees, but linked to the National Risk Assessment (NRA). We raised with HMRC that the NRA assess Money Service Businesses as high risk due to the ongoing concerns around money transmitters, however travel money is low risk. We have also asked them to consider a tiered approach to premises fees, e.g. the first 2,000 subject to the highest fee, which would take into account the economies of scale of supervision of large traders like Post Office. Such a solution would also ensure HMRC meets the requirements of 'Managing Public Money Guidance' whereby they must ensure that smaller businesses are not subsidising the supervision or larger businesses. They have agreed to explore these points, and a further meeting is planned in July.
- 69 The F&P system solution was delivered on 12th June and data migration from the current solution scheduled for completion by end June. The project team is working on processes and controls with Post Office teams to ensure that there are no missing fields from source data for the monthly feeds into the new system. The re-declaration process is due to commence in July, with monthly HMRC reports being driven from the new system from the July submission. We have written to HMRC and asked that we change the submission date to the fourth Friday each month, and are awaiting their response.

External Threats

- 70 The National Crime Agency (NCA) published the 2020 National Strategic Assessment of Serious and Organised Crime. It emphasises that UK-based criminals are continuing to introduce criminal cash into the UK banking system. Criminals are utilising money mules, money service businesses, post offices and virtual assets as a means of disguising the origins of their cash as it enters the financial system.
- 71 Throughout the lockdown period, we have continued to see high levels of suspicious banking cash deposits, and continue to work with the National Economic Crime Centre (NECC) and Project Admiralty (one case involves high value cash deposits made onto multiple banks cards at 45 branches between 18th February and 8th June 2020 totalling c.£7m). A further meeting has been held with the banks in the Banking Framework sub group that is looking at money laundering risks, but there is little progress on identifying control improvements to date. A further meeting is planned for July.
- 72 We continue to support the Covid Fusion Cell, and a sub group has been established to look at cash based money laundering. Criminals continue to exploit the COVID-19 posing as employees of government authorities and legitimate businesses. Phishing emails and phone calls have involved requesting payment for treatment, fake websites selling testing kits, vaccines and masks. The NECC expects that the UK will see an increase in fraud related to COVID-19 over the coming months, and there is particular concern about the effect that the downturn on the economy will have on criminals being able to more easily recruit mules to launder the proceeds of crime. The Financial Crime team have delivered a number of branch communications to increase branch awareness of scams and COVID-19 related fraud, and further communications are planned.

Supply Chain Compliance



- 73 No assessment visits undertaken since March. Awaiting sign off by the Health and Safety team for a re-start date to commence assurance visits - expected to commence in July, provided there is available accommodation.
- 74 Twice-weekly communications were issued to sites during April and May to help maintain compliance, 12 were issued in total.
- 75 Weekly compliance activities focussing on specific areas of assurance activity commenced in June and will run until the end of July.

Financial Services

Compliance Monitoring

- 76 Compliance is currently supporting the business with support and communications on preparing for business re-invigoration in the post lockdown environment.
- 77 The key resumption of activity will be branch travel insurance sales (potentially in September). This will require compliance oversight of training, awareness and communications (including brochure ware) and eventually monitoring. This will be a significant undertaking particularly with new Covid 19 travel insurance policy restrictions that will need to be disclosed clearly at point of sale.
- 78 Mystery shopping was paused in March. We are planning to introduce a small number of mystery shops from August for POI protection business and it is likely that wider mystery shopping (BoI, Telecoms) will resume in Q3, including for the re-launched travel insurance business.
- 79 We continue to maintain governance and regular 'check ins' with our Principals. The normal monthly governance meetings have remained in place albeit with a reduced level of MI.

FS Regulatory updates

- 80 A summary slide of the key future developments is included in the reading room, a number of planned changes have been delayed whilst the regulator focuses on managing the crisis. The immediate focus from the FCA during Covid 19 crisis has been working with the industry on the well published consumer forbearance measures for credit card, loan and mortgage repayments, these are being delivered through our product partners BoI and Capital One.
- 81 A key focus area has also been regarding retaining access to cash for the vulnerable particularly as the growth of contactless payment has continued. We await the government legislation on this, but in the meantime the FCA stated in June that they have been working closely with firms to help them move towards reinstating services for customers in a consistent way. The expectation is that firms will prioritise;
- 82 Where possible, and in line with relevant government guidelines, reinstating access to cash and essential services in local areas which have lost access to bank branches or cash during the crisis.
- 83 Where it is not possible to reinstate access, and in areas where a reduced service remains, ensuring that there is clear communication to customers through websites and physical signs at branches to signpost to alternatives, such as Post Office services.

Digital Accessibility Compliance

- 84 The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018 come into force for public sector websites including Post Office from 23



September 2020 and PO Mobile Apps from 23rd June 2021. The purpose of these rules is to improve digital accessibility for vulnerable and disabled customers. Post Office will also need to publish an accessibility statement on our website explaining how accessible the site is.

- 85 The D&I team have been working for some time with an external accessibility auditor AbilityNet to provide compliance support and to audit the Post Office website. AbilityNet are established leaders in their field and have worked with a number of large public and private sector firms.
- 86 D&I have focussed on key areas of our website that will have the most customer interaction and traffic. The D&I team and AbilityNet have confirmed that this approach is consistent with the approach taken by other public sector bodies.
- 87 The audits have raised a number of issues, (e.g., such as colour contrast, being able to tab instead of using a mouse) but the intention is to fix as many of them as possible against the audited pages and modules. By doing so we intend to lodge ourselves, with backing of AbilityNet our third party auditor, as partially compliant as opposed to fully compliant, because we have focused our attention on a series on significant touchpoints on our website, as opposed to the entire digital product, for the reasons outlined above.
- 88 The Government Digital Service (GDS) will examine a sample of public sector websites every year. GDS can ask for information and request access to intranets, extranets or any public sector website. Significant non-compliance could be seen as a breach of the Equality Act 2010 and the Disability Discrimination Act 1995.
- 89 However, Post Office has a credible work plan in place with improvements made and in progress, including the use of external accessibility experts and expected involvement and support with the charity sector.
- 90 Legislation dictates that we have until 23rd June 2021 to meet compliance for any mobile applications, and on completion our web accessibility programme, the D&I team will be conducting the same activity against the app to meet that deadline.

Mails – Dangerous Goods

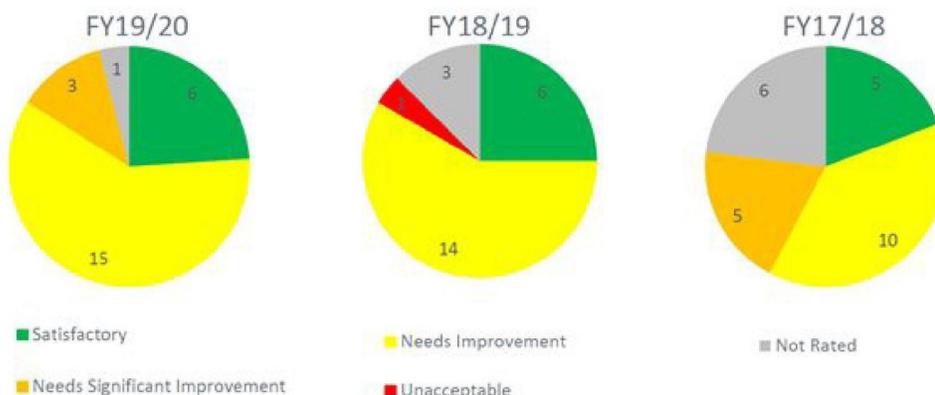
- 91 Please refer to the separate paper included in the Reading Room. This paper sets out, in detail, the activities being developed by the Mails and Network Teams, in conjunction with Royal Mail.



Internal Audit

Summary of Control Environment and Control Themes for 2019/20:

92 The distribution of report ratings for the past three years indicates that the overall control environment has remained stable and suggests a gradual improvement over time.



93 The lower number of audit findings further indicates an improvement in the control environment. During 2019/20 Internal Audit raised a total of 171 audit actions across 25 audits (compared to 271 actions across 24 audits in 2018/19).

94 Audit findings were analysed to identify recurring control themes and root causes. An exact comparison from year to year isn't possible due to the varying subject matter covered by each year's audit plan, however, it signals the direction of travel for key control components. The top five control themes are shown below, with full results included in the reading room (Appendix 8).

Control Theme (by COSO control components)	% of Audit Findings		
	19/20	18/19	
<u>Change Delivery</u> ⁽¹⁾ : Ineffective change governance, risk management and tracking / realisation of benefits.	31%	44%	↓
<u>Control Activities</u> : Internal controls are not deployed through policies, procedures and systems and / or internal controls are not designed or operating effectively.	22%	15%	↑
<u>Risk Assessment</u> : Ineffective identification and/or management of operational, financial and information risk (including unclear expression of risk appetite).	13%	5%	↑
<u>Information & Communication</u> : Unavailability of relevant, quality information to support the internal control function and decision making.	8%	12%	↓
<u>Monitoring Activities</u> : Oversight and governance groups are not effective in identifying and correcting control weaknesses.	6%	3%	↑

⁽¹⁾ Change Delivery is not a standard COSO control component, however, findings from Change Assurance reviews are shown separately to avoid distortion of BAU controls.

11



95 The year-on-year movements in control themes can be summarised as follows:

- **Change Delivery:** There was a notable improvement in the effectiveness of Change governance and controls. A significantly lower number of control failings were identified compared to the previous year (53 vs 118), from a similar number of reviews performed. The reorganisation of the Strategic Portfolio Office (SPO) and appointment of a new Chief Transformation Officer in 2019, together with the adoption of a Change Excellence Framework have laid the foundations for a stronger control environment driven centrally by the SPO. A detailed Change Controls Framework has also been developed, and although this is still being embedded, there is already a noticeable improvement in the consistency and effectiveness of controls operating at programme level.
- **Control Activities:** The percentage of audit findings relating to ineffective control activities has increased by 7 percentage points, indicating reduced effectiveness of core internal controls and is a regression from the 18 percentage point improvement reported the previous year. Our audits have noted that control activities did not always keep in step with organisational and system changes, in particular process and control documentation required updating. We highlight that appropriate remediation was implemented for all control failings which were identified. We will assess the role of the second line of defence activities to monitor first line controls operation – there are 3 reviews of the second line on the FY20/21 plan.
- **Risk Assessment:** Operational risk management was less effective compared to the previous year (findings increased from 5% to 13%). Risks were not always proactively identified, remediated and escalated.
- **Information & Communication:** There has been an improvement in availability of relevant, quality information to support the internal control function and decision making (down to 8% from 12%). The standard of policies and procedures continue to improve, with more effective communications to raise awareness of new or updated policies.
- **Monitoring Activities:** Although this represents a low number of findings (10 instances or 6% of total findings), the year on year deterioration indicates that oversight and governance groups have become less effective in identifying and correcting control weaknesses. This could be a consequence of staff churn, especially at a senior level where monitoring activities will typically be led and challenged by more experienced managers.

11

Audit report turnaround performance for 2019/20

96 The average time to clear internal audit reports during 2019/20 improved significantly from 41 days the previous year to 30 days (against a target SLA of 20 days). The improvement was achieved despite the delays experienced in the clearance of the final reports for 2019/20 due to the impact of Covid-19.



Progress against Internal Audit plan

97 At the time of the May ARC meeting, the last audit from the 2019/20 internal audit programme was still being finalised. This report (FS Branch Sales) has since been completed and a summary is included in par 101.



- 98 In response to the Covid-19 crisis, a re-prioritised Internal Audit programme was approved at the May ARC meeting. It was agreed that a more dynamic (quarterly rolling) audit plan will be adopted and reviewed at each ARC. Progress against the Q1 plan is shown in the table below with the full plan in the reading room (Appendix 16):

	Review	Status & Timing
POL		
1	Covid-19 Programme Assurance	Final report issued. In addition Deloitte delivered 3 insight reports to ARC.
2	Maintain Minimum Control Standards	Two interim reports issued (Cash Controls and Financial Reporting Controls). Third and final phase (IT Controls) – final draft report with management for review.
3	Cyber Security Maturity	Final report issued.
4	Health & Safety response to Covid-19	In progress (30/6 – 30/7).
5	Effectiveness of Second Line during Covid-19	Interim report issued. Phase 2 (deep dive) in progress (12/7 – 30/7).
POI		
6	Data: Governance, ethics, privacy & security	Phase 1 underway to assess 3 rd Party Data Security Risks.
7	Cyber Security (POL-POI Gap Analysis)	In progress. Fieldwork nearing completion (17/6 – 24/7)
8	Incident and Breach Management	In progress (17/6 – 24/7)

- 99 The following audits are being planned for delivery in Q2 & Q3:

	Review	GE Sponsor	Timing
1	GLO Operations Improvement Programme (Common Issues Judgement)	Julie Thomas	Oct
2	DB Pension Scheme Data Errors	Lisa Cherry	July
3	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Sept
4	GLO Historical Shortfall Scheme - Data Validation	Amanda Jones	July
5	Controls over Revenue Adjustments	Al Cameron	Aug
6	Branch Hub (Programme Assurance)	Al Cameron	Sept
7	Belfast Exit (Programme Assurance)	Jeff Smyth	Oct

11

Internal Audit reviews completed

- 100 The following six audit reports were issued since the May ARC meeting:

1	FS Branch Sales (FY20 IA Plan) (Final Report)	Green	4	Minimum Control Standards - Ph1 Cash Controls	Green
2	Effectiveness of Second Line during CV-19 – Ph1	Grey	5	Minimum Control Standards – Ph2 Financial Reporting Controls	Yellow
3	CV-19 Programme Assurance - Ph1 Set-up & Governance	Green	6	Cyber Security Maturity Assessment	Yellow

- 101 Our findings and observations from these reports are summarised below, with the full reports available in the reading room (appendices 9-15).



1. FS Branch Sales (Ref. 2019/20-25)



Satisfactory

Sponsor:
Owen Woodley

Audit actions:

P1	0
P2	0
P3	1
Total	1

Appendix 9

The objective of this review was to assess the adequacy and operating effectiveness of controls to ensure that promotional materials offered and activities undertaken in branch in support of FS product sales are compliant with the AR agreements and the related regulatory requirements.

We conclude that the mechanisms in place to assure branch sales compliance, are operating as described, which enables Post Office to meet its contractual obligations to its Principals. IA noted significant improvements in the processes and controls operating when compared with those reviewed previously in FY16/17. In addition, we highlight that the risk exposure has been reduced since FY16/17 as sales activities are now limited to a subset of PO Money products, along with travel and some protection insurance sold on behalf of POI. We noted an opportunity to review Post Office’s assurance approach to ensure it remains fit for purpose and is done in a cost effective way.

Management Comment
We welcome the satisfactory rating and will continue working with our principals, network and compliance colleagues to ensure our mechanisms and approaches remain as effective as they can be.
Chrysanthy Pispinis – Post Office Money Director

Network welcomes the findings and recommendations of this report. As a result of the new field team structure implemented in March 2019, which extended our reach to all physical branches, the network has significantly strengthened its Financial Services compliance awareness.
Andy Kingham – Head of Network

I am pleased the review recognises the strengths in Compliance’s oversight of FS branch activity and the approach taken. We continue to develop our approach to oversight and this will include any changes required to support the developing branch distribution strategy.
Jonathan Hill – Compliance Director

2. Effectiveness of the Second Line (Ph1) (Ref.2020/21-07)

Not Rated

Sponsor:
Al Cameron / Ben Foat / Jeff Smyth

Management comments and audit actions will be in the final report at the end of phase 2.

Appendix 10

The objective of this review is to assess if key second line assurance activities continue to operate effectively during the Covid-19 crisis. Internal Audit have completed an initial assessment of the impact of Covid-19 on 12 second line assurance activities in Post Office.

Results from our initial assessment indicate that all second line functions continued to operate effectively throughout the Covid-19 crisis. Teams are able to work remotely, have clear priorities and are generally positive about their interactions with the business, senior and external stakeholders. However, some teams are facing significant additional challenges and will be subject to a more in-depth review to understand if, and to what extent, their effectiveness has been impaired.

Based on the results of phase 1 of this review we will perform a more in-depth review of the following five second line activities: Loss Prevention, Financial Crime, Compliance, IT Security and Health & Safety.

11



3. Covid-19 Response Programme (Ref. 2020/21-06)									
 <p>Satisfactory</p> <p>Sponsor: Nick Read</p> <p>Audit actions:</p> <table border="1"> <tr> <td>P1</td> <td>0</td> </tr> <tr> <td>P2</td> <td>2</td> </tr> <tr> <td>P3</td> <td>2</td> </tr> <tr> <td>Total</td> <td>4</td> </tr> </table> <p>Appendix 11</p>	P1	0	P2	2	P3	2	Total	4	<p>The Covid-19 Programme was established following the Business Protection Team’s early mobilisation and crisis response to the pandemic during February and March 2020. The programme was key to formalising the management of the next stage of crisis relief activities whilst supporting Post Office objectives.</p> <p>The objective of this review was to provide in-flight and ongoing assurance to the programme with focus on programme organisation, governance and oversight.</p> <p>We concluded that the set-up, and management of the Covid-19 programme has been effective in driving Post Office’s mobilisation and crisis response activities. The programme objectives were clear and its scope was intentionally broad to give operational flexibility to the crisis response, which was carefully managed and the budget tightly controlled. Overall the programme has achieved its objectives, which included delivery of a significant number of operational improvements to BAU.</p> <p>Our review has identified some areas for improvement, however, we don’t believe that these weaknesses were significantly detrimental to the work being carried out in response to Covid-19. With the programme progressively moving toward closure, the noted weaknesses should be included as lessons learned for future Covid-19 waves or other crisis response programmes. The lack of a formal, comprehensive, data model for the Network MI dashboard should also be addressed prior to the programme closure.</p>
P1	0								
P2	2								
P3	2								
Total	4								
<p><u>Management Comment provided by Caroline Scott – Portfolio Director – Organisation Effectiveness</u></p> <p>The Covid-19 Programme was established to lead and manage Post Office’s immediate / first 3 months response to the Covid-19 pandemic with clear guiding principles to:</p> <ul style="list-style-type: none"> • Support communities: put our customers, postmasters, colleagues at the heart of our decision making • Protect the elderly, the vulnerable and those who are sick or dealing with bereavement • Ensure business and team resilience to deal with mass absenteeism and provide relief • Follow Government guidelines unless this does not make commercial sense for POL • Apply the human touch – empathy, recognition and celebration of the small things that make a difference to our daily lives • Recognise that actions speak louder than words to build Pride and Trust in our Post Office brand <p>Against the crisis backdrop, clear programme governance and a dedicated programme team ensured the focus to follow a “people led” approach. This recognised that Post Office had a key worker role to support communities and the people who relied on us through its postmasters, keeping branches open and services available whilst keeping its colleagues and customers safe and secure. The programme team built pride and trust in what it was delivering every day through collaboration, fast decision making and actions, managing key risks and making a difference. This created a very positive team culture and way of working which it will be important not to lose as lockdown eases. Importantly, the closure of the programme ensures appropriate handover into BAU and clear governance to stand up the programme again should Covid-19 alert levels change.</p>									



4. Minimum Control Standards (Ph1) Cash Controls (Ref. 2020/21-05)	
 <p>Sponsor: <i>Al Cameron</i></p> <p>Management comments and audit actions will be in the final report at the end of phase 3.</p> <p><i>Appendix 12</i></p>	<p>The purpose of this audit was to consider the impact on key controls from changes in processes as a result of operational challenges arising from Covid-19, and to ensure that minimum control standards are operating effectively. Phase 1 of this review assessed controls over cash processes. We have rated this report satisfactory, having concluded that controls over cash were appropriate in the circumstances and continued to operate effectively during the response to Covid-19.</p> <p>From the outset, Supply Chain knew it would be affected by staff absence due to shielding, self-isolation and sickness, which at its height reached up to 30%. New controls with contingency suppliers were put in place to ensure the distribution of outbound cash and the reconciliation of inbound cash could be processed in a timely fashion. This involved working with both Loomis and NatWest to agree the level of services and ensure adequate levels and standards of control could be applied to all processes. Good collaboration across businesses and teams enabled this to be done very quickly and the contingency arrangements were working within the first two weeks of April.</p> <p>Supply Chain also introduced a risk based single-pass check for processing of inbound remittances to enhance productivity (resulting discrepancies are being closely monitored).</p> <p>A request from DWP to send cash to the most vulnerable of POCA customers was responded to with similar efficiency, using Royal Mail Special Delivery. Controls have been devised and implemented to ensure this service can be offered securely and on demand whilst safeguarding the personal data of vulnerable customers.</p> <p>Controls over the normal cash processes have been operating as designed throughout the crisis with minimal interruption. Where changes have been necessary to accommodate remote working these have been defined, agreed, signed off appropriately and implemented. The audit highlighted a need to improve controls documentation and audit trail.</p>

5. Minimum Control Standards (Ph2) Financial Reporting Controls (Ref.2020/21-05)	
 <p>Sponsor: <i>Al Cameron</i></p> <p>Management comments and audit actions will be in the final report at the end of phase 3.</p> <p><i>Appendix 13</i></p>	<p>The purpose of this audit was to consider the impact to key controls from changes in processes as a result of operational challenges arising from Covid-19, and to ensure that minimum control standards are operating effectively.</p> <p>Based on our work to date, we conclude that the control environment relating to Financial Reporting has been maintained throughout PO's response to the Covid-19 crisis, albeit with challenges around formally evidencing control activity. Controls have been operated as if in BAU for the most part and only amended where absolutely necessary to accommodate the challenges of a remote working population.</p> <p>The control self-assessment process has been maintained throughout, although there were access issues with TrAction that delayed the evidencing of controls operation for April. This has now been resolved.</p> <p>We further highlight opportunities to improve controls over Agent Expenses and Payroll processes that were designed to operate in the office environment, particularly in relation to evidencing checks and manager authorisation. These controls have had to be adapted for the remote working environment, but do not permit an adequate audit trail to be maintained. Management are implementing MS Teams to evidence control activity and retain audit trail.</p>



6. Cyber Security Maturity Assessment (Ref.2020/21-02)



Sponsor:
Jeff Smyth

Audit actions:

P1	4
P2	4
P3	0
Total	8

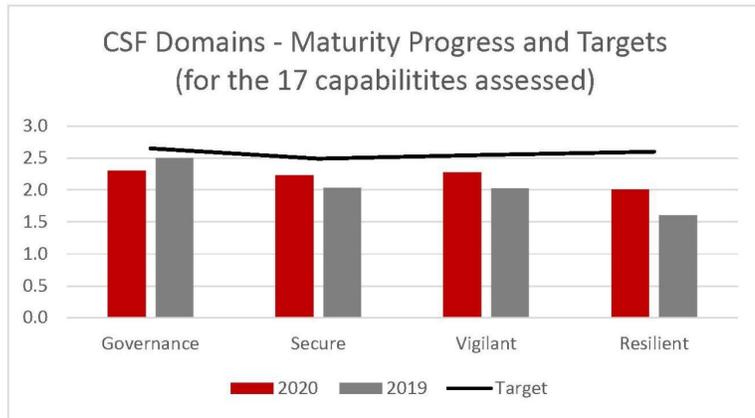
Appendix 14 & 15

In 2018/19, Deloitte, in partnership with Internal Audit, carried out a comprehensive review of Post Office’s cyber controls across 34 cyber capabilities. The objective of this review was to re-assess the maturity of controls in place to protect the confidentiality, integrity and availability of POL’s infrastructure, systems and data.

Significant work has been carried out over the last year to rationalise the cyber operating model and enhance controls, especially those which protect data and identify threats and vulnerabilities. Policies and standards now better reflect the individual controls needed to meet requirements, POL’s ability to capture and act on threat intelligence is greatly enhanced, and progress has been made on managing the identity lifecycle through integration of HR and IT systems.

However, we highlight that further work is required to meet target maturity levels and there is a need to develop and document a comprehensive strategy and architecture to support the deployment of cyber security. This should be focused around an agreed set of Crown Jewels and lead into an end-to-end cyber programme.

The graph below shows the change in maturity of the four Cyber domains, for the 17 key capabilities which were selected for re-assessment. It also shows that, despite the good progress in most capabilities, maturity still falls short of the maturity targets set in 2019.



We have rated this report '**Needs Improvement**', reflecting the progress made against the maturity targets and an assessment of the degree to which cyber risks are mitigated by the current controls.

The overarching report with agreed audit actions and Deloitte’s executive summary report are included in the reading room as appendices 14 and 15. The full Deloitte report (96 pages) is available on request.

Management Comment provided by Tony Jowett (CISO)

This review has been focused on the areas where we believe we have made some progress positively and also where we are highlighting areas that need further activity. The review scores, the comments associated with them and the development activity highlighted are fair and accurate.



Status of Audit Actions

102 Audit actions are generally being completed on time. However, we highlight that the changes to business priorities due to Covid-19 have caused delays in completion of some audit actions. We have been working with the action owners and GE sponsors to agree revised completion dates for 14 actions and we will continue to track progress for these actions against the revised dates. Six of these actions are now delayed beyond the revised date - explanation provided below.

103 The movement and ageing of audit actions are shown in the table below (status at 17 July 2020).

Audit Action Status (POL):		Ageing:	
Open actions at last ARC	54	Open (not yet due)	40
<i>Less:</i> Actions closed in period	28	Overdue (<60 days)	8
<i>Add:</i> New actions in period	22	Overdue (>60 days)	0
Total open actions	48	Total open actions	48

104 The reasons for the 8 overdue actions are as follows:

Belfast Exit Programme – Covid-19 delayed the re-start of the Belfast Exit programme, which impacted completion of 8 audit actions. These actions are now being addressed following the approval from IC to continue with programme delivery. Internal Audit will review progress with the actions during August when we will perform our pre-work for the next phase of the programme (Action owner: Rob Wilkins, GE Sponsor: Jeff Smyth).



Appendices²

Central Risk

- Appendix 1: Enterprise, Intermediate and Risk Register Dashboards
- Appendix 2: Change Portfolio

Compliance

- Appendix 3: Prohibited Restricted Items
- Appendix 4: Covid-19 Dashboard
- Appendix 5a: Compliance Dashboard
- Appendix 5b: Compliance Dashboard
- Appendix 6: Telecoms Regulatory Calendar
- Appendix 7: FS Regulatory Calendar

Internal Audit

- Appendix 8: 2019/20 Internal Control Themes Summary
- Appendix 09: Internal Audit Report – FS Branch Sales
- Appendix 10: Internal Audit Report – Effectiveness of Second Line during CV-19 (Ph1)
- Appendix 11: Internal Audit Report – Covid-19 Programme Assurance (Ph1)
- Appendix 12: Internal Audit Report – Minimum Control Standards (Ph1) Cash Controls
- Appendix 13: Internal Audit Report – Minimum Control Standards (Ph2) Financial Controls
- Appendix 14: Internal Audit Report – Cyber Security Maturity Assessment (IA Summary)
- Appendix 15: Internal Audit Report – Cyber Security Maturity Assessment (Deloitte Report)
- Appendix 16: Internal Audit Plan for 2020/21

² Appendices are accessible in the CoSec 'Reading Room'