

Royal Mail Group

Compliance with Legislative & Regulatory Obligations

Post Office Limited

Internal Audit & Risk Management

Internal Audit Report: 07/083

February 2008



Royal Mail - CONFIDENTIAL

Contents & Distribution

Contents

Executive Summary	Page 3
Detailed findings	4
Appendices	
Appendix A - Legislation & regulation impacting on POL and potential impact of breach	6
Appendix B- Control Assessment Framework	7
Appendix C - Risk profile based on self-assessment of level of control	8
Appendix D - Adjusted risk profile	9
Appendix E - Compliance framework suggested outline contents	10
Appendix F - Impact and likelihood scoring frame	11

Distribution

Executive Summary & Appendices

Alan Cook, Managing Director, Post Office Ltd (POL)
Post Office Ltd Executive Team
Clive Bradley, Head of Property Projects
Nick S Gittens, Head of Diversity & CSR
Jackie Hesley, Head of Industrial Relations
Alwen Lyons, Head of Mails Services Marketing
Andy Z McLean, Head of Operations Control
Keith Rann, Head of Supply Chain
Penny Slatter, Head of Direct Sales
Clare Wardle, Head of Post Office, Legal Services
Keith Woollard, Head of Compliance

Executive Summary

Royal Mail Group Executive Team
Doug Evans, General Counsel
Derek K Foster, Internal Audit & Risk Management Director
Ernst & Young, External Auditors

Internal Audit & Risk Management Team

Shaun Delaney, Maxime X Allen

Executive Summary: Overview

Background

Whilst the POL Compliance Team provide a focus for regulated products, this does not extend to other aspects of legislative and regulatory obligations. The Group Compliance Director and Post Office Limited (POL) Head of Compliance have voiced concerns regarding the adequacy of the control environment across the range of legislation and regulation that impacts on POL. In addition, the strategic risk profile developed by the POL Executive Team identifies failure to comply with our statutory and regulatory obligations as an area of risk.

Objectives & approach

The overall objective is to provide an assessment of the risk that POL does not comply with its statutory or regulatory obligations and provide tools to support the business unit in the ongoing assessment, monitoring and management of this risk. Specific objectives are to: identify the key gross risk exposures; facilitate an assessment of control effectiveness around the most significant exposures; and provide an overall net assessment of risks and identify priorities for improving the application of a compliance framework in POL.

The approach identified all areas of legislation and regulation that impact on POL and, through consultation with Legal Services and the Head of Compliance, produced from this a list of key areas for POL, excluding areas managed entirely at Group level. Nominated members of the Executive Team and Senior Leadership Population were asked to self-assess controls in these areas using a questionnaire previously developed and used at Group level, but modified for POL as agreed with the Head of Compliance. The self-assessment was compared with information provided by Legal Services.

Rating

AREA CONTROL ENVIRONMENT: there is a **MEDIUM** risk of POL breaching its statutory and regulatory obligations.

RISK TO GROUP: LOW. There are no significant risks that have a Group impact.

Key findings

Control Environment. Managing the impact of legislation on POL is complex with policies mostly, but not exclusively, owned at Group level and responsibility for deployment in POL often spread across different functions. POL is embraced by the Royal Mail Group Compliance Framework, which is specifically focused on RM Licence Conditions and Competition Law. However, given the wider trend towards an increasing regulatory burden, the breadth of legislation impacting on POL and the complexity of the control environment required to manage its compliance, it would be appropriate for POL to develop its own compliance framework. We have provided an outline of such a framework that sets out accountabilities, controls and governance processes to deliver an adequate control environment across the range of legislation and regulation. Specific matters on which controls are self-assessed generally as insufficient, and which would be improved by incorporating them into a compliance framework, are compliance monitoring and staff awareness and understanding of their responsibilities.

Controls Self-Assessment Perception Gap. The self-assessments of controls to enable compliance suggest a high level of control. However, in many areas of legislation the Legal Services' view, based on judicial reviews, litigation history, compensation claims and dialogue with regulators, suggests that the self-assessments, taken as a whole, are not fully reliable. This "perception gap" may itself create a risk if it leads to failure to take action when it would be appropriate to do so. An adjusted risk profile that reflects apparent gaps in perception of controls and also Legal Services' assessment of the degree of regulatory scrutiny shows, overall, a higher level of risk compared with that derived from self-assessment.

Specific Aspects of Legislation. The principle areas of legislation or regulation where the risk of non-compliance is highest are:

- Personal data protection where POL products are being transacted by third party suppliers such as POFS;
- Public Procurement Legislation, reflecting the newness of control measures implemented and concerns about overall levels of awareness.

Self-assessments are not available for a number of areas, two of which warrant particular attention: Competition Law, breach of which could have a severe financial impact; and copyrights and trademarks legislation, which offer opportunities to protect POL's intellectual property assets.

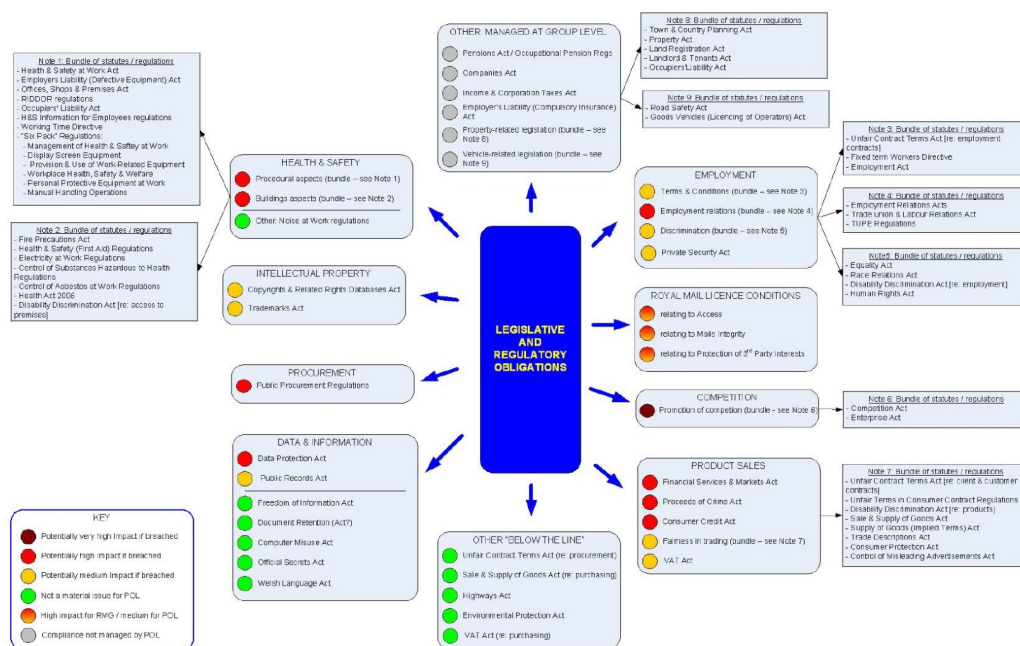
Detailed findings

The following issues were identified during the review and the corrective action and timescale were agreed with the business. All of the actions shown are deemed important. However, a further ranking (1-2) has been provided to assist in prioritisation. Priority 1 relates to the higher risk issue.

Issue	Agreed Action Plan	Action Owner	Timing
<p>1. Control environment</p> <p>1.1 Compliance framework</p> <p>POL does not have its own compliance framework; it applies an RMG compliance framework, but the coverage is limited to compliance with the RM Licence and Competition Law.</p> <p>1.2 Compliance controls</p> <p>1.2.1 Priority areas for improvement</p> <p>The self-assessment exercise indicates that the priorities are: compliance monitoring; staff awareness of their responsibilities; further work to ensure policies owned by POL are fully fit-for-purpose. Development of an effective compliance framework would address these matters.</p> <p>1.2.2 Business change</p> <p>The established change control process enables legislative and regulatory issues to be identified at an early stage in any business change, but deployment is inconsistent: for example some strategic initiatives have not gone through change control. There is activity currently in hand that will increase compliance with the process as part of the current business planning round.</p> <p>1.3 Controls perception</p> <p>There is 'perception gap' between the self-assessment of controls to manage legal and regulatory obligations and POL's litigation record and losses history, and concerns raised by regulatory bodies.</p> <p>1.4 Link with Critical Business Processes (CBPs)</p> <p>Compliance with Legal and Regulatory obligation is a CBP for POL, which was most recently self-assessed as "substantially deployed". However, the CBP is specifically concerned with processes that apply to product-related regulatory compliance rather than legislation and regulation in general.</p> <p>Business impact</p> <ul style="list-style-type: none"> Absence of an overall framework creates an inconsistent approach to compliance. Over-estimating the strength of control may lead to complacency and may itself create a risk to compliance. 	<p>1. Develop and communicate an appropriate compliance framework for POL to cover all key aspects of legislation identified in this review. (Priority 2)</p> <p>2. Review the portfolio of CBPs in light of the control enablers identified in the self-assessment questionnaire used in this review, and, if appropriate, amend the portfolio (Priority 2)</p>	<p>Keith Woollard</p> <p>Keith Woollard</p>	<p>31 Dec 2008</p> <p>31 Dec 2008</p>

Detailed findings

Issue	Agreed Action Plan	Action Owner	Timing
<p>2. Areas of legislation or regulation where the risk of non-compliance is high</p> <p>2.1 Data Protection Act (DPA) as it applies to sales via direct channels.</p> <p>The self-assessment raised a specific concern that it is not clear who is responsible for setting standards that POL expects third party suppliers, including POFS, to adhere to and for ensuring such standards are met. Further, there is no monitoring of third party compliance performance in place. The risk to reputation is especially high given the current levels of public interest following several high profile instances elsewhere of failure to protect personal data. Adoption of a POL specific compliance framework will make responsibility clear.</p> <p>2.2 Public Procurement Legislation (PPL).</p> <p>Although controls are self-assessed as high, recent history, which includes a "Letter before Action" from the regulatory body requiring appropriate controls to be put in place, suggests that the control environment, established in December 2007, is not mature and the Legal Services' view is that awareness and understanding of this legislation are not yet well established.</p> <p>Business impact</p> <ul style="list-style-type: none"> • Breach of data protection obligations may cause reputation damage that undermines POL's drive for growth in Financial Services product sales. • Breach of PPL obligations may result in awarded contracts having to be re-tendered with subsequent delays to projects or product developments. 	<p>3. Review contractual relationships with third party suppliers and introduce the provision of DPA conformance; develop a action plan to address any gaps that are identified,</p> <p>(Priority 2).</p>	<p>David Glynn</p>	<p>31st Aug 2008</p>
<p>3. Incomplete self-assessment</p> <p>Self-assessment questionnaires were not completed for a number of areas of legislation; and without these the risk assessment is incomplete. Amongst the areas not self-assessed are:</p> <ul style="list-style-type: none"> • Competition Law. This is an important area to review since the impact of the breach could be very high – the law allows for a fine of up to 10% of turnover • The law relating to copyrights and to trademarks. These areas are important in that effective control will allow POL to ensure that its own intellectual property assets are adequately protected. Therefore, these represent an opportunity as well as a potential risk. <p>Business impact</p> <p>Failure to complete the self-assessment may mean that areas of non-compliance with adverse financial consequences, and also potential opportunities afforded by the legislation are overlooked.</p>	<p>4. Complete the outstanding self-assessment questionnaires and forward them to IA&RM who will use them to update the charts provided in this report</p> <p>(Priority 2).</p>	<p>Gary Hockey-Morley</p>	<p>31st May 2008</p>

Legislation & regulation impacting on POL and potential impact of breach Appendix A

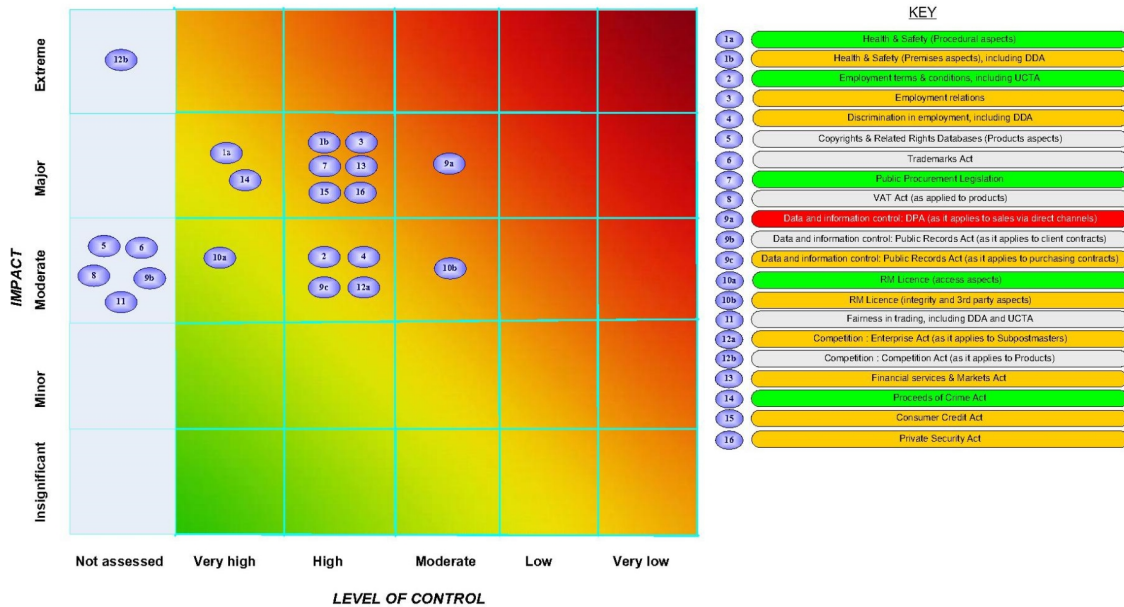
Control assessment framework

Appendix B

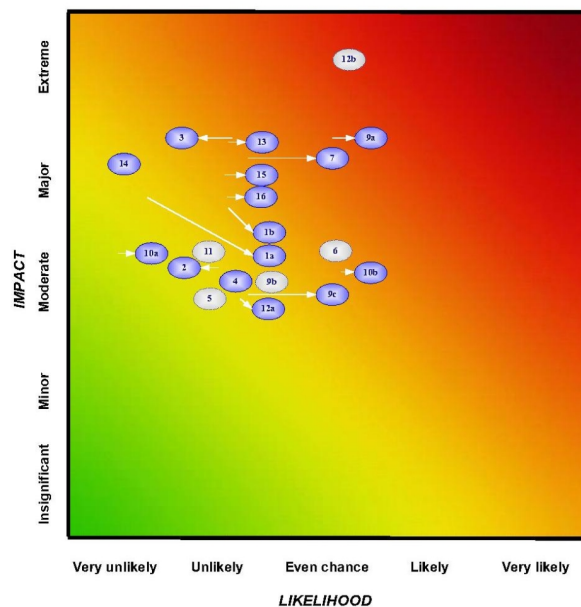
CONTROL ENABLERS		Leadership - 20%		Policies & Strategy - 10%		People - 15%		Partnerships & Resources - 15%		Processes - 20%		Monitoring & Assurance - 20%		Control Assessment		Assessment based on litigation experience	Perception gap	Level of regulatory scrutiny			
Ref No	CONTROLS CAPABILITIES Legislation / regulation	ET / SLP Self-assessment provider	Clear and active Board level accountability	Clear and active responsibility amongst senior managers	Policy in place and fit for purpose	Compliance requirements are clearly defined and deployed	Employee responsibilities defined in job descriptions	Assessment programmes effectively deployed	Clear & effective disciplinary procedures for non-compliance	Adequate and effective resources and expertise	Effective supplier management	Adequate use of and support from skilled corporate oversight function(s)	Legislative / regulatory requirements are embedded into Operational Procedures	Effective identification and evaluation of new legislative developments	Effective integration of legislative obligations into new product/producer projects				Effective monitoring & management information systems / audit trail	% Score	Self-assessed overall Level of Control
1a	Health & Safety (Procedural aspects)	Nick Gilems via Toby Manskin	4	4	N/A	N/A	4	4	4	4	N/A	4	4	4	4	4	100.00%	Very High	Moderate	Red	Medium
1b	Health & Safety (Practical aspects), including OGA	Clive Brindley	4	3	N/A	N/A	4	4	4	3	3	4	3	3	3	3	83.33%	High	Moderate	Amber	Medium
2	Employment terms & conditions, including UCTA	Jackie Lesley via Toby Manskin	4	4	4	4	2	3	4	4	4	4	4	4	4	2	86.25%	High	High	Green	Low
3	Employment relations	Jackie Lesley via Toby Manskin	4	4	4	4	1	3	4	4	4	4	4	4	4	2	85.00%	High	High	Green	Low
4	Discrimination in employment, including OGA	Nick Gilems via Toby Manskin	4	4	N/A	N/A	1	3	4	4	4	4	4	4	4	4	94.44%	High	Moderate	Amber	Low
5	Copyrights & Related Rights (Database Act, as it applies to PCL products)	Gary Hockey-Money																Moderate	NA	NA	Very low
6	Trademarks Act	Gary Hockey-Money																Low	NA	NA	Very low
7	Public Procurement Legislation	Andy McLean via Keith Gann	4	3	N/A	N/A	3	4	2	4	4	4	4	4	4	2	81.94%	High	Low	Red	Medium
8	VAT Act (re products)	Gary Hockey-Money																	Not assessed	NA	Medium
8a	Data and information control - DPA as it applies to sales via direct channels	Penny Statter	3	4	N/A	N/A	2	4	4	1	2	4	4	4	4	0	65.25%	Moderate	Moderate	Green	High
8b	Data and information control - PRA as it applies to client contacts	Gary Hockey-Money																	Moderate	NA	Low
9a	Data and information control - PRA as it applies to purchasing contracts	Andy McLean via Keith Gann	4	4	N/A	N/A	0	3	3	4	4	4	4	4	4	4	91.67%	High	Moderate	Amber	High
10a	ISM Licence (access aspects)	Alwen Lyons	4	4	4	4	4	4	4	4	4	4	4	4	4	4	100.00%	Very High	Very High	Green	Very high
10b	ISM Licence (integrity and 3rd party aspects)	Paula Vennells	3	3	2	3	2	3	3	3	2	4	3	3	3	2	67.50%	Moderate	Moderate	Green	Very high
11	Fairness in trading, including OGA and UCTA	Gary Hockey-Money																	High	NA	Medium
12a	Legislation promoting competition - Enterprise Act, as it applies to Subcontractor relationships	Paula Vennells	4	4	3	3	4	3	3	4	4	4	4	4	4	3	96.00%	High	Moderate	Amber	Medium
12b	Legislation promoting competition - Competition Act, as it applies to PCL products	Gary Hockey-Money																	Moderate	NA	Medium
13	Financial Services & Markets Act	Keith Woolford	4	3	3	4	3	3	3	4	4	4	4	4	4	3	85.33%	High	High	Green	High
14	Proceeds of Crime Act	Keith Woolford	4	4	3	4	3	4	4	4	4	4	4	4	3	4	95.83%	Very High	Very High	Green	Medium
15	Consumer Credit Act	Keith Woolford	3	3	3	4	4	3	3	4	4	4	4	3	4	3	95.83%	Very High	High	Green	Medium
16	Financial Security Act	Keith Rann via Paula Money	4	3	2	4	2	3	4	4	N/A	4	4	4	4	4	90.79%	High	High	Green	High
Average			3.8	3.6	3.1	3.8	2.6	3.4	3.3	3.7	3.6	4.0	3.9	3.7	3.8	2.9	86.69%	High	Moderate	Amber	
KEY Self-assessment scoring guidelines		4 Control fully deployed / embedded as business as usual If Yes this is the way we do business or strongly aligns with this document		3 Control (partially) in place but not fully deployed or Yes this usually happens but should be improved or Yes it aligns with this document, but some issues to improve		2 Control is under development / review or Yes it happens occasionally, but there is no consistency		1 No records of the need for this control or planned to do this only happens with this document		0 The need for this control has not been recognised in this document		N/A This control is not applicable to PCL or the context of this regulation		Abbreviations • OGA: Disability Discrimination Act • DPA: Data Protection Act • PRA: Public Records Act • UCTA: Unfair Contract Terms Act							

Risk profile based on self assessment of level of control

Appendix C



Adjusted risk profile



Appendix D

KEY

1a	Health & Safety (Procedural aspects)
1b	Health & Safety (Premises aspects), including DDA
2	Employment terms & conditions, including UCTA
3	Employment relations
4	Discrimination in employment, including DDA
7	Public Procurement Legislation
9a	Data and information control: DPA (as it applies to sales via direct channels)
9c	Data and information control: Public Records Act (as it applies to purchasing contracts)
10a	RM Licence (access aspects)
10b	RM Licence (integrity and 3rd party aspects)
12a	Competition: Enterprise Act (as it applies to Subpostmasters)
13	Financial services & Markets Act
14	Proceeds of Crime Act
15	Consumer Credit Act
16	Private Security Act

Possible risk status for other areas of legislation for which self-assessment has not been completed based on information provided by Legal Services, including degree of regulatory scrutiny

5	Copyrights & Related Rights Databases (Products aspects)
6	Trademarks Act
9b	Data and information control: Public Records Act (as it applies to client contracts)
11	Fairness in trading, including DDA and UCTA
12b	Competition: Competition Act (as it applies to Products)

Note: arrows show adjustment from the self-assessed position based on:
? volume and value of litigation and losses history
? dialogue with regulatory authorities
? Legal Services' perception of the degree of regulatory scrutiny

Colour coding of risk exposures is in line with the impact and likelihood scoring frame provided at Appendix F

Suggested outline of a compliance framework**Appendix E**

1. Introductory statement from the Managing Director defining legislative and regulatory compliance and setting out the importance of compliance.
2. Scope: Areas of legislation and regulation that are applicable to POL, and distinguishing between key legislation / regulation and other, as per Appendix B of this report.
3. Accountability for each key area of legislation / regulation:
 - If there is a RM Group level policy, the framework to identify: policy owner; policy reference and details of how to access it; ET level "champion" who leads on deploying the policy in POL; contact point for queries;
 - If there is a POL business policy, the framework to identify: policy owner (ET level "champion"); policy reference and details of how to access it; contact point for queries.
4. Controls. The framework sets out generic responsibilities for the ET level "champion" to ensure that appropriate controls are in place:
 - all staff and managers for whom this item is relevant, including new entrants and transferees, to be aware of how the law might impact on them and what their responsibilities are (it may be possible to prepare as an Appendix to the framework a matrix of staff / manager groups and relevant legislation);
 - procedures are in place to ensure that all relevant managers and non-managers are kept informed of changes in requirements;
 - staff awareness is monitored periodically and supported by training where appropriate;
 - there is sufficient specialist and non-specialist resource to manage and monitor compliance with legislative obligations;
 - legislative risks impacted / generated by supplier dependencies or by clients have been identified;
 - suppliers are clear about what is expected of them to support and ensure compliance with the legislation and this is reflected in supplier contracts;
 - appropriate use is made of Legal Services' and other Corporate oversight functions' advice in non-routine situations in which there is potential for non-compliance, and to explore and exploit opportunities for competitive advantage provided by the legislation / regulation;
 - there are appropriate procedures in place to ensure that the implications of new / emerging legislation are identified, evaluated and responded to appropriately and in a timely manner;
 - operating procedures are designed to meet the requirements of the legislation / regulation and appropriate POL or RMG policy;
 - procedures exist to ensure that Legal Services' and other Corporate oversight functions', as appropriate, are consulted in the development of new products, business processes and projects (cross-referring to the business change process, how this is a tool to manage compliance and requirement for conformance);
 - monitoring systems are in place to assess compliance with the legislation / regulation, and to identify and track remedial action where performance falls short.
5. Governance. Compliance with legislative and regulatory obligations is a CBP and is subject to periodic self-assessment and independent validation, which is signed off by the Managing Director and reported to the Corporate Risk Management Committee bi-annually, which enables the business to provide its statutory declaration on risk and control in its annual report.
6. Statement that disciplinary measures will be applied for wilful, persistent or negligent non-compliance, and a cross-reference to the RMG Whistleblowing policy which is available for suspected wilful non-compliance
7. Contact point for queries about the framework and for initial queries about specific aspects of legislation where it is not clear from Section 3 (suggestion: Head of Compliance to be this contact point).
8. Sign-off by Managing Director.

Impact and likelihood scoring frame

Appendix F

LIKELIHOOD		
No	Descriptor	Guidelines
5	Very likely	Expected to occur in most circumstances (greater than 90% chance)
4	Likely	Will probably occur in most circumstance (71-90% chance)
3	Even chance	As likely to occur as not (21-70% chance)
2	Unlikely	Not generally expected but could occur at some time (5-20% chance)
1	Very unlikely	Expected to occur only in exceptional circumstances (less than 5% chance)

IMPACT						
No	Descriptor	Financial (POL impact)	People	Political	Customer Service	Reputation
5	Extreme	Asset / profit or potential opportunity loss of more than £20m	Death of more than one person	Government enquiry into operational inadequacies or financial loss	National service disruption at major locations for more than 20 days	Prolonged national media coverage
4	Major	Asset / profit or potential opportunity loss of £5m-£20m	Death of one person	Repeated concerns or complaints raised in Parliament, by public groups or industry associations	National service disruption at major locations for between 1 and 20 days	National media coverage
3	Moderate	Asset / profit or potential opportunity loss of £1m-£5m	Serious injury to more than one person	Concerns or complaints raised by public groups or industry associations to Government bodies	Regional service disruption for up to 10 days	Regional media coverage
2	Minor	Asset / profit or potential opportunity loss of £100k -£1m	Serious injury to one person or any injury to more than one	Concerns or complaints raised by public groups or industry associations to local government	Local (single site) disruption for 1-3 days	Local press coverage
1	Insignificant	Asset / profit or potential opportunity loss of less than £100k	Injury resulting in certificated sick absence	Local operational issues raised with member of Parliament	Service disruption less than 1 hour	Letters to the editor, local press

