ARTICLE:

The Post Office IT scandal – why IT audit is essential for effective corporate governance

By James Christie

Introduction

The Post Office Horizon scandal has unfolded over more than two decades. The original IT development started in 1996. In 2019 some 550 former subpostmasters, subpostmistresses and former Post Office employees (for convenience together here referred to as 'SPMs') were successful in two preliminary issues in group litigation (a civil claim) brought by them against the Post Office.[1] In the second of those judgments, the trial judge, Mr Justice Fraser, concluded that the claimants' case was substantially correct. He found that the Post Office's Horizon computer system had a propensity, because of errors and bugs in it, to cause the kind of shortfalls and alleged losses that SPMs had experienced, and for which they were in many cases prosecuted by the Post Office for offences of dishonesty. He also found that the Post Office and Fujitsu exercised powers of remote access to SPM terminals without their knowledge. This judgment is not the end of the story. There remains a number of questions: how the scandal happened, who should be held accountable, and if so by whom, and how the victims should be compensated.

My experience working as an IT auditor in financial services means that I have taken a particular interest in the Post Office's corporate governance, and the question of whether the board of directors and the executives responsible for exercising that governance discharged their duties and responsibilities.

Bugs are not simply a result of errors in writing code. A bug is conventionally thought of in software testing as being something that causes a system to behave in a way that a user does not expect. It includes usability issues and many other factors, as Mr Justice Fraser noted in the Horizon Issues trial:[2]

> 'Software bug means something within a system that causes it to cause an incorrect or unexpected result
>
> …
>
> Bugs, errors or defects is not a phrase restricted solely to something contained in the source code, or any code. It includes, for example, data errors, data packet errors, data corruption, duplication of entries, errors

[1] The Justice for Subpostmasters Alliance (https://www.jfsa.org.uk/) obtained funding for these actions from Therium Group Holdings Limited: https://www.therium.com/ ; *Bates v Post Office Ltd ((No 3) Common Issues))* [2019] EWHC 606 (QB) and *Bates v The Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB).

[2] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), [26]-[27], http://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html .

in reference data and/or the operation of the system, as well as a very wide type of different problems or defects within the system.'

The presence or absence of management controls over the system and the corporate culture play an important role in both the number and seriousness of the bugs that are created. They also shape the way that the corporation responds to bugs and deals with them. The response can be constructive, or it can be harmful to the corporation. Both the existence of software bugs and the way that they are handled, once identified, fall within the remit of those engaged in corporate governance.

It is clear that the Post Office consistently failed to apply its corporate governance processes effectively. In particular, Internal Audit failed to meet the professional standards expected of them, both by the corporation and by the profession. That failure has continued over a period of more than two decades. It started when Royal Mail owned the Post Office and provided an audit service. It continued after the Post Office separated from Royal Mail and created its own Internal Audit function. Under both regimes the internal auditors, and in particular the IT auditors, failed to respond to clear warning signs that there were serious problems with the Horizon system. The failings were so serious that they raise concerns about whether the Royal Mail and Post Office had sufficient competent IT auditors.

The Post Office Horizon IT inquiry 2020

The Horizon IT system controls the accounts of some 11,500 Post Office branches around the United Kingdom. Between 2000 and 2013 the Post Office prosecuted 736 people,[3] many of whom protested their innocence (though many entered pleas of guilty to fraud to avoid prosecution for theft and in the hope of a non-custodial sentence). The prosecutions pushed some of the supposed perpetrators into financial ruin, ill health, and even suicide. A number of SPMs who were affected by prosecutions, civil proceedings and other enforcement action by the Post Office formed the Justice for Subpostmasters Alliance (JFSA). They joined together in group litigation under a Group Litigation Order made by the court in 2017 and, in due course succeeded in two preliminary issues in that group litigation against the Post Office that were tried as preliminary issues before the individual claims were to be heard.[4] The judgment in the second case was particularly damaging for the Post Office, in which the trial judge determined that Horizon was seriously flawed and that it had prosecuted hundreds of SPMs on the basis of evidence that was incomplete, inaccurate or unreliable.

As the ultimate owner of the Post Office, the UK government, was forced to act. In September 2020 the Department for Business, Energy & Industrial Strategy (BEIS) announced that Sir Wyn Williams would chair the non-statutory Post Office Horizon IT Inquiry, which would start work immediately. On 19 May 2021 Paul Scully, Parliamentary Under-

[3] The Final Reckoning, https://www.postofficetrial.com/2021/04/the-final-reckoning.html .
[4] The first trial is reported at *Bates v Post Office Ltd ((No 3) Common Issues)* [2019] EWHC 606 (QB), http://www.bailii.org/ew/cases/EWHC/QB/2019/606.html .

Secretary at BEIS, announced that the Williams' Inquiry would be converted into a statutory inquiry.[5] The associated press release confirmed the commitment made at the launch of the non-statutory inquiry that it would establish 'a clear account of the implementation and failings of Horizon over its lifetime'.[6] The Inquiry's terms of reference[7] made it clear that the scope would extend beyond the IT system itself and include the Post Office's corporate governance. Section F states:

> 'F: Examine the historic and current governance and whistleblowing controls in place at Post Office Ltd, identify any relevant failings, and establish whether current controls are now sufficient to ensure that failing [sic] leading to the issues covered by this Inquiry do not happen again.'

The phrase 'at Post Office Ltd' seems restrictive. A full examination of corporate governance must lead the inquiry to consider the conduct of BEIS, and also UK Government Investments Limited (UKGI), through which BEIS owns the Post Office (as its sole shareholder). Interestingly, section F of the terms of reference for the non-statutory inquiry had previously been slightly different:[8]

> 'F: Examine the governance and whistleblowing controls now in place at Post Office Ltd and whether they are sufficient to ensure that the failings that led to the Horizon case issues do not happen again.'

The amended terms of reference make it clear that the inquiry must look at the historical controls over corporate governance. As I shall explain, the failings in corporate governance were an important contributory factor in the development of the scandal and in the reluctance by the Post Office to accept what happened. The new terms of reference also opened up the examination of failings in corporate governance to include any that were relevant to the scope of the inquiry. The previous version had referred, possibly ambiguously, to 'failings that led to the Horizon case issues'. This could have been interpreted as covering only the corporate governance failings that were related to the fifteen Horizon issues examined by Mr Justice Fraser in *Bates v Post Office Ltd (No 6: Horizon Issues)*. That would have seriously curtailed the effectiveness of any review of corporate governance at the Post Office.

The present government might maintain that the failings at the Post Office occurred largely before the current government came to power. While such a contention may be understandable, over time there has been a consistent pattern of unwillingness to accept responsibility by several governments including the present. The current government clumsily involved itself by setting up an inquiry with limited powers and scope. The inevitable result was widespread suspicion that the government intended there to be a highly restricted inquiry that avoided the most important issues, perhaps seen as politically sensitive. The decision to put the Inquiry on a statutory footing, and to

[5] Post Office Update, Statement made on 19 May 2021 by Paul Scully (UIN HCWS40), https://questions-statements.parliament.uk/written-statements/detail/2021-05-19/hcws40 .
[6] Government press release, 'Government strengthens Post Office Horizon IT inquiry with statutory powers', https://www.gov.uk/government/news/government-strengthens-post-office-horizon-it-inquiry-with-statutory-powers .
[7] Post Office Horizon IT inquiry 2020: terms of reference: https://www.gov.uk/government/publications/post-office-horizon-it-inquiry-2020/terms-of-reference .
[8] Update on Post Office Horizon IT Inquiry, Statement made by Paul Scully Statement on 30 September 2020 (UIN HCWS477), https://questions-statements.parliament.uk/written-statements/detail/2020-09-30/hcws477 .

amend the terms of reference, gives Sir Wyn the opportunity to perform a full scrutiny of what went wrong with corporate governance at the Post Office.

The wording of section F now commits the Inquiry to examining the historic and current controls in place, and whether they are sufficient to prevent a repeat of the scandal. The Post Office has had an elaborate and credible framework for corporate governance in place for over a decade. It was in place well before some of the most serious governance failings occurred, yet it neither prevented nor exposed them. The corporate governance of the Post Office failed SPMs, and it failed the taxpayer, which will now have to provide financial support, because the Post Office and government have publicly stated that it will be unable to meet the level of compensation claimed under the Historic Shortfall scheme established following the Horizon Issues judgment.[9] That disregards claims by those who have had their convictions subsequently quashed by appeal courts. The controls were in place, but the management commitment that was necessary to make them effective was missing, as discussed in this article. Any investigation of the Post Office scandal must look carefully at how the board and executives managed corporate governance over the decades of the Horizon scandal, and that must bring the actions of the ultimate owner, the UK government, which is represented on the board, within the scope of the inquiry.

The failure to reveal the problems

The three aspects of the Post Office's corporate governance that interest me are: (i) risk management, (ii) the internal audit function, and (iii) whistleblowing. All three are linked. The Post Office's risk management failed catastrophically over the Horizon system. Internal Audit should have detected that failure of risk management and supported any whistleblowing. If necessary, which it was, Internal Audit should have acted as whistleblowers themselves, as is discussed below.

The risks of financial and reputational damage to the Post Office arising from the Horizon system and the risk that a defective IT system might harm the SPMs were not identified and were therefore not managed. Reading through the succession of annual reports issued since the Post Office was split off from Royal Mail in 2012, it might seem that the Horizon scandal was an unforeseen event that took the corporation by surprise. But the Horizon risks are exactly the sort of risks that an effective risk management framework should handle. That framework should have been overseen and monitored by Internal Audit.

The explicit inclusion of 'whistleblowing controls' within the scope of the inquiry is interesting. Scrutinising governance necessarily entails an examination of the whistleblowing processes and responsibilities. That the Inquiry's scope includes 'governance and whistleblowing controls' emphasises that point. A striking feature of the history of the Horizon system is the abundance of internal evidence that was available over many years to justify the

[9] Paul Scully, Parliamentary Under-Secretary (Department for Business, Energy and Industrial Strategy), Post Office Update Statement, 18 March 2021 (Statement UIN HCWS853), https://questions-statements.parliament.uk/written-statements/detail/2021-03-18/hcws853 .

external concern about the quality of the system, but not a single employee or officer publicly raised this until long after they had stopped working for either the Post Office or Fujitsu.

Establishing what went wrong with the Horizon system will require an understanding of why the corporate governance processes, controls and safeguards failed to protect the corporation, the taxpayers, and above all the SPMs.

Corporate governance – how it should be done

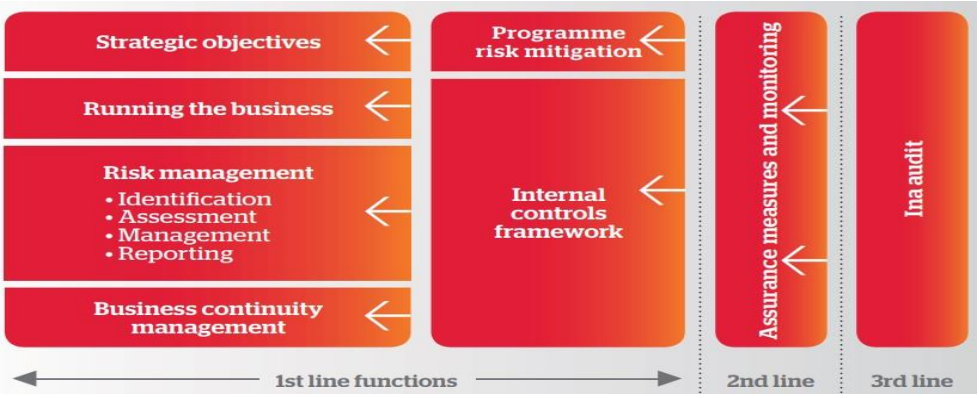
The Three Lines of Defence

In order to understand how the Post Office's corporate governance functions failed, it is important to understand what they should have done. Section 4, 'Audit, Risk and Internal Control' of the UK Corporate Governance Code states the following principles:[10]

> 'M. The board should establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements.
>
> N. The board should present a fair, balanced and understandable assessment of the company's position and prospects.
>
> O. The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.'

Applying such principles of good governance within a corporation requires a framework of processes and responsibilities. The Three Lines of Defence is a reputable model for providing the risk management component of corporate governance and it is recommended by the Chartered Institute of Internal Auditors (IIA).[11] It has been followed widely since it was developed in the 1990s for KPMG at the HSBC bank. The Royal Mail adopted it before the Post Office was split off in 2012. The Post Office has continued to use it ever since and describes the model in its annual reports, as set out below.

[10] Financial Reporting Council, 'The UK Corporate Governance Code', 2018, https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.pdf .
[11] Chartered Institute of Internal Auditors, 'Position paper: The three lines of defence', https://www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence/ .



The Three Lines of defence, as illustrated in the Post Office Annual Report, 2013. *There is a typographical error in the third line. It should read 'Internal Audit'.*[12]

The first line of defence involves operational management applying the agreed controls, risk management, and security measures. The second line is provided by specialist risk management, compliance, and security functions. The third line is the independent assurance that internal audit offers to the board that the whole model is working effectively. This crucial third line of defence failed at the Post Office. There were clearly other serious failings, but Internal Audit should have provided the independent assurance that these problems had been detected and managed responsibly. This third line of defence, the final backstop, should have alerted the Board if all else had failed.

The power of internal audit

People who have never worked in corporate internal audit are often surprised at the power, independence and freedom of action that internal auditors enjoy in an organization that takes corporate governance seriously. When I was an IT auditor for a major UK insurer, my login account had a powerful privilege that meant I had what is called 'read access' to all data. This allowed us to start investigations instantly and discreetly, without seeking permission through the normal route. Audit management monitored the use that we made of the facility.

Another illustration of the wide-ranging power of an auditor was our ability to demand immediate support from technical experts for urgent investigations, such as apparent fraud. People in important roles could be required to take part or cooperate with an investigation. In practice this power had to be used diplomatically, but in my experience, there was never any argument if we used the conventional polite formula 'I'm afraid we need X for a couple of days to work on a confidential matter.' If a manager demurred, we would say 'I'm sorry – but I will have to insist', and the person we needed would join our investigation. The people whose knowledge and expertise we needed were invariably quite content to be asked to stop their routine work and take on an interesting challenge.

[12] Post Office Limited, 'The fabric of our society - Annual Report and Financial Statements 2012-13', https://web.archive.org/web/20211201221351/https:/corporate.postoffice.co.uk/media/44158/annualreport1213.pdf .

The Post Office's internal auditors have this same conventional range of powers, notably with 'unfettered access to staff, data and systems'. The corporate website helpfully confirms this in the ARCC's Terms of Reference:[13]

'The Committee shall:

30. Approve the appointment or termination of appointment of the Head of Internal Audit.

31. Approve the Internal Audit Charter every two years. (Footnote. The purpose of the charter will be to grant Internal Audit unfettered access to staff, data and systems required in the course of discharging its responsibilities to the Committee. It will also ensure it has sufficient resources to fulfil its mandate and will require audits to be completed to appropriate professional standards, aligning with the requirements of the Institute of Internal Auditors.)

32. Review and approve the annual Internal Audit Plans, including any changes to these plans, to ensure they are aligned to the key risks of the business and review reports on work carried out. The review should include methods employed by the internal auditors to assess risk and to prioritise the various audit proposals identified in the annual plan.

33. Ensure internal audit has unrestricted scope, the necessary resources and access to information to fulfil its mandate.

34. Ensure the Internal Auditor (i.e. Head of Internal Audit) has direct access to the Board Chair and to the Committee Chair and is accountable to the Committee.

35. Monitor and review annually the effectiveness of the internal audit function in the context of the Group's overall risk management system and the work of compliance, finance and the external auditor and as part of this assessment:

i. Meet with the Head of Internal Audit without the presence of management.

ii. Review the annual internal audit plan work and results.

iii. Determine whether it is satisfied that the quality, experience and expertise of internal audit is appropriate for the business.

iv. Review actions taken by management to implement the recommendations of internal audit and to support the effective working of the function.

36. Ensure the independence of the internal auditor including an annual review of any non-audit services provided by internal audit.

37. Determine whether an independent, third party review of processes is appropriate.'

[13] Post Office Audit, Risk & Compliance Committee Terms of Reference, https://corporate.postoffice.co.uk/media/anab51ea/20210604_pol_arc_gov_termsofreference_approved_final.pdf .

The reference to Internal Audit 'discharging its responsibilities to the Committee' is significant. Internal Audit reports to the ARCC and the Terms of Reference makes it clear that the ARCC is independent of executive management, as set out in paragraph 61:

> 'The Committee shall consist of at least two independent non-executive directors and only independent non-executive directors shall be eligible to be members of the Committee. The Chair of the Board shall not be a member of the Committee.'

These provisions confer very considerable power, freedom of action and independence from corporate management. Good internal auditors cannot be intimidated or threatened because they have a direct reporting line to a committee made up of non-executive directors. Executive management cannot dismiss internal auditors acting responsibly.

Internal Audit must ensure that its work is aligned to the 'key risks of the business'. The ARCC is responsible for reviewing the way that Internal Audit assesses risk and prioritises its audits (paragraph 32). The ARCC must also 'monitor and review annually the effectiveness of the internal audit function in the context of the Group's overall risk management system' (paragraph 35). Paragraphs 23 to 26 give the ARCC and Internal Audit powers and responsibilities that are striking in the light of the Horizon scandal. The ARCC was explicitly responsible for the whistleblowing process and also for monitoring cases of fraud and the way that they were handled:

> 'Compliance, Whistleblowing and Fraud.
>
> The Committee shall:
>
> 23. Review with the internal auditors and the external auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing.
>
> 24. Review at least annually the adequacy and security of the Company's arrangements for its employees and contractors to raise concerns, in confidence, about possible wrongdoing in financial reporting, regulatory breaches or other matters. The Committee shall determine that these arrangements allow proportionate and independent investigation of such matters and appropriate follow up action.
>
> 25. Review the Group's procedures for detecting fraud and the systems and controls for prevention of bribery and any non-compliance.
>
> 26. Review any summary of frauds, thefts and other irregularities of any size.'

It is worth quoting the ARCC's Terms of Reference in detail to show how much power and responsibility it, and Internal Audit, had to scrutinize the actions of Post Office executives and the risks to which the corporation was exposed by the board and executive. The footnote to paragraph 31 is particularly significant. This commits Internal

Audit to complying with the standards and requirements of the IIA. Those requirements provide the benchmark against which the performance of the internal auditors can be measured. The Post Office Internal Audit function failed to meet the prescribed standard. Evidence of this failure is provided by the long list of warning signs which did not elicit an adequate response from the internal auditors at Royal Mail and the Post Office.

The red flags of warning

The Three Lines of Defence provides a sound basis for corporate governance; but it cannot ensure, still less guarantee, the effective management of risk. That requires proactive, competent, responsible managers who take the framework seriously. Regardless of the processes that are in place, any corporate governance framework is ineffective if those charged with governance responsibilities fail to respond to warning signs of impending risk.

In the case of the Post Office and its Horizon system, there were clear and obvious red flags over more than two decades, extending to a decade before the Post Office was split off from Royal Mail. A brief account of the most glaring warnings is worthwhile:

1999 Three cabinet ministers offered trenchant criticism of the original Horizon project and the quality of the system before the Select Committee on Trade and Industry.[14] The ministers were Alistair Darling (Secretary of State for Social Security), Alan Milburn (Chief Secretary to the Treasury) and Stephen Byers (Secretary of State for Trade and Industry). The reason for three ministers being involved was that the original Horizon system was intended to permit payments of benefits via smartcards at Post Office branches. The system did not work, and altered to remove the smartcards and benefits payments, leaving it as an internal accounting system for Post Office branches.

Alan Milburn said: 'the contractor … under-estimated the complexity of the contract. They under-estimated the scale of the project too. They under-estimated the risks inherent in it ...'

Alistair Darling offered a verdict that looks ominous 22 years later: '… there were hundreds of problems with it in terms of inaccuracy and difficulty ... No-one else in the world is using this sort of technology.'

Under-estimation, complexity, risk, inaccuracy, difficulty; these are all words that should attract the attention of IT auditors. However, the most startling observation is Darling's comment about nobody else using the same technology. Early adopters of technology often pay a heavy price in problems and poor quality ('bleeding edge').[15] There can be commercial advantages for a fast-moving company adopting new technology. The benefits are less obvious for a public sector organization, and the balance of risks would normally suggest a stable, proven solution would be more prudent.

[14] Select Committee on Trade and Industry, Minutes of Evidence, Examination of Witnesses (Questions 138 - 159), 14 July 1999, https://publications.parliament.uk/pa/cm199899/cmselect/cmtrdind/530/9071402.htm .
[15] 'Bleeding edge technology', Wikipedia. https://en.wikipedia.org/wiki/Emerging_technologies#In_the_media.

2002 At [32] of the Technical Appendix to *Bates v The Post Office Ltd (No 6: Horizon Issues) Rev 1*, Fraser J cites text from a Technical Environment Description, dated 22 October 2002:

> 'The system architecture … is not based on conventional client-server models. Nor does it conform to traditional central-system models. It adopts an entirely original and highly innovative four-tier model …'.
>
> '… Not based on conventional client-server models', 'original and highly innovative'. These are phrases that are attractive in advertisements, but which worry experienced IT auditors. It was a further confirmation that the Horizon system was not using well-established technology but was at the risky 'bleeding edge'.

2009 Internal memorandums revealed that there were objections within the Post Office to obtaining data from Fujitsu about Horizon which the defence in criminal prosecutions had requested. The reluctance was because the contract with Fujitsu required the Post Office to pay for this data.[16] IT auditors would regard such information as being essential to understanding how the system was working. They should take a critical view of any contract that entailed an additional charge to see it. Such an arrangement would raise concerns about whether the system was controlled effectively.

Computer Weekly ran a story in May 2009 about 'bankruptcy, prosecution and disrupted livelihoods' being inflicted on SPMs.[17] The article's standfirst[18] was 'Rebecca Thomson reports on claims that the Post Office has failed to recognise a potential IT problem.'

This article was one of an increasing number of articles in the press, notably *Private Eye* and *Computer Weekly*, both of which followed the story relentlessly. The interest taken by *Computer Weekly* was particularly significant. It is a prominent trade journal, copies of which are often to be found scattered around IT installations. There are few media outlets that would have had greater effect amongst IT workers, whether in development or audit.

Accountancy Age reported in October 2009 on the mounting concerns that Horizon had flaws which misstated branch accounts.[19] The article quoted a senior representative of the Institute of Chartered Accountants in England and Wales, and it stated that the newspaper asked the Post Office whether it would perform an IT audit of Horizon. Richard Anning, head of the ICAEW IT faculty,[20] said: 'You need to make sure

[16] *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, [91], http://www.bailii.org/ew/cases/EWCA/Crim/2021/577.html .
[17] Rebecca Thomson, 'Bankruptcy, prosecution and disrupted livelihoods - Postmasters tell their story', 11 May 2009, https://www.computerweekly.com/news/2240089230/Bankruptcy-prosecution-and-disrupted-livelihoods-Postmasters-tell-their-story .
[18] A 'standfirst' is the introductory summary to a newspaper article. It is written in a bolder, larger type in order to attract attention.
[19] Rachael Singh, 'Post Office is urged to act over IT concerns', Accountancy Age, 8 October 2009, https://www.accountancyage.com/2009/10/08/post-office-is-urged-to-act-over-it-concerns .
[20] The IT Faculty of the Institute of Chartered Accountants in England and Wales was established in 1991: 'The faculty provides products and services to help members and other business professionals make the best possible use of IT. It helps members

that your accounting system is bullet proof.' He added: 'Whether they have an IT audit or not, they need to understand what was happening.' It is reported that the Post Office declined to comment when asked if it would undertake an IT audit. *Accountancy Age* also attached an editorial comment to the story: '*The Post Office should consider an IT audit to show it has taken the matter seriously. Although it may be small sums of money involved, perception is everything and it could not consider going back into bank services with an accounting system that had doubts attached to it.'*

2010 In August Rod Ismay, the Post Office's Head of Product and Branch Accounting, issued a report, 'Horizon – Response to Challenges Regarding Systems Integrity'.[21] Ismay expressed complete confidence that Horizon was robust and warned against any independent investigation:[22]

> 'It is also important to be crystal clear about any review if one were commissioned – any investigation would need to be disclosed in court. Although we would be doing the review to comfort others, any perception that POL doubts its own systems would mean that all criminal prosecutions would have to be stayed. It would also beg a question for the Court of Appeal over past prosecutions and imprisonments.

The fear that commissioning an independent investigation would imply a lack of confidence in the Horizon system suggests that Post Office management had closed minds on the subject of the quality of Horizon and were unwilling to risk discovering anything that might disturb their confidence. That would have sent a clear, and harmful, message to those whose job it was to investigate the integrity of IT systems.

The Ismay report has a particularly interesting section, 'Independent Review and Audit Angles'. This makes it clear that the purpose of any independent investigation would be to persuade others of Horizon's reliability. It makes no mention of Internal Audit being involved in the discussions, unlike the Press Office:

> 'POL has actively considered the merits of an independent review. This has been purely from the perspective that we believe in Horizon but that a review could help give others the same confidence that we have.

keep up to date with information technology issues and developments. It also represents chartered accountants' IT-related interests and expertise and contributes to IT-related public affairs.' The faculty was renamed the Tech Faculty in 2019: https://www.icaew.com/library/historical-resources/guide-to-historical-resources/technical-releases-and-representations/releases-and-representations-on-information-technology .

[21] Editorial note: This Report was cited in the Court of Appeal and is in the public domain, but it is not available on the internet. One of the editors (Stephen Mason) wrote to Nick Vamos, a Partner at Peters & Peters Solicitors LLP acting for Post Office Limited, requesting a copy of the Ismay Report. Mr Vamos kindly sent a copy, redacted for the purposes of privacy, which is the same version disclosed to the Court of Appeal. In thanking Mr Vamos, the editor explained the Report will be published in the Documents Supplement of the journal for 2022; please cite as: Post Office Limited Ismay Report, 19 *Digital Evidence and Electronic Signature Law Review* (2022), Documents supplement.

[22] *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, [24].

> Our decision between IT, Legal, P&BA, Security and Press Office has continued to be that no matter what opinions we obtain, people will still ask "what if" and the defence will always ask questions that require answers beyond the report. Further such a report would only have merit as at the date of creation and would have to be updated at the point at which Horizon or the numerous component platforms were upgraded.
>
> Ernst & Young and Deloittes are both aware of the issue from the media and we have discussed the pros and cons of reports with them. Both would propose significant caveats and would have limits on their ability to stand in court, therefore we have not pursued this further.'

Ruling out an investigation by external auditors on the grounds that they would insist on caveats, and limit what they would say in court is certainly noteworthy and does not seem consistent with a responsible approach to prosecution. It is also remarkable to see an argument that an independent report 'would only have merit as at the date of creation'. There is some superficial truth in that statement; system audits do report on a system at a point in time. It is, however, highly misleading. The argument applies only to an audit report which has found no faults and made no recommendations. I have never seen such a report. A report listing faults is relevant until the faults are corrected and re-tested, and it explains how the system has performed up to the point of the audit.

The list of recipients of the report is significant. It was issued to fourteen senior managers, including the Post Office's Managing Director, the Head of IT, the Heads of the Criminal and Civil law teams and the Head of Security, but not Internal Audit.[23] The omission of Internal Audit is puzzling. The internal auditors should have been a vital source of independent assurance within the corporation. It would have been their job to conduct any internal investigation of the sort that would justify senior managers' confidence, yet it seems that they were not given a copy of the report. That raises a question. What was the basis for senior management's confidence in Horizon if it was not provided by Internal Audit?

2010 It was revealed during the Common Issues trial[24] in 2018 that the Post Office knew in September 2010 that the system had a bug which meant that the central system could record a discrepancy for a branch, even though the branch terminal had told the subpostmaster that the account was balanced perfectly (the 'receipts and payments mismatch' bug). This bug was discussed in a memorandum circulated widely within the Post Office and Fujitsu in August 2010, including Post Office Finance and Security.[25] Nevertheless, the Post Office persisted with its practice of holding SPMs liable for any discrepancy on the grounds that the figures produced by Horizon were totally reliable.

[23] Nick Wallis, *The Great Post Office Scandal*, (Bath Publishing, 2021) page 136.
[24] *Bates v Post Office Ltd ((No 3) Common Issues))* [2019] EWHC 606 (QB).
[25] Nick Wallis, 'Post Office internal memos: Serious Horizon errors', 2018, https://www.postofficetrial.com/2018/11/two-important-documents.html .

2011 In the management letter accompanying the annual audit report in March 2011, the Post Office's external auditors, Ernst & Young (E&Y) drew attention to continuing weaknesses in IT governance and control in the outsourced IT service provided by Fujitsu.[26] In particular, E&Y drew attention to the need for greater control over privileged users. It was revealed in the Horizon litigation in 2019 that these weaknesses continued to be unaddressed and unresolved up to 2015. This is highly significant in the light of the Post Office's insistence that it was impossible to amend branch data remotely (i.e. not from within a branch);[27] many of the IT support staff were permanently assigned powerful privileges to allow them to amend branch data.[28]

Such 'superuser' IDs[29] are tightly controlled in a well-managed IT installation. Having external auditors point out such a serious weakness of management control of this kind should be extremely embarrassing for any Internal Audit department. It is very surprising, and inexplicable, that the weaknesses that were clearly identified and important were not addressed immediately.

Mr Justice Fraser agreed that the controls and auditing associated with these IDs were inadequate. In his judgment, this pointed to a clear failure in corporate governance. It is hard to reach any other conclusion given that the problem was not resolved in the four years after it was reported by the external auditors:

> '[694] What this amounts to, in my judgment, is a serious deficiency both in the required level of controls in Horizon, in the recording of what privileged users were actually doing (other than that they were simply logged on) and also a corresponding absence of recording and auditing of those activities.'

2012 The forensic accounting firm Second Sight Support Services Limited was commissioned to investigate the Horizon system following the bad publicity, Parliamentary pressure, and the campaigning of the JFSA. Second Sight provided an Interim Report,[30] which referred to the existence of bugs in the Horizon system and queried sums paid by the Post Office into suspense accounts without the source of the money being identifiable. Second Sight raised the possibility that Horizon itself might be the cause of problems. Following this report, the Post Office undertook a review of its prosecutions. Mrs Paula Vennells, formerly CEO of the

[26] Ernst & Young, 'Post Office Limited Management letter for the year ended 27 March 2011', (August 2011), https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/document_24_-_ernst___young_llp_management_letter_for_the_year_ended_27_march_2011_1.pdf .

[27] Ian Henderson and Ron Warmington. 'Initial Complaint Review and Mediation Scheme: Briefing Report Part Two'. Second Sight Support Service Ltd, 2015. [14.6]; https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/document_34_-_second_sight_final_briefing_report_part_two_1.pdf .

[28] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), [390]-[394]; Dr Robert Worden (Post Office witness). 'Well, we are aware that the APPSUP role is powerful and we are aware that the SSC [Fujitu's Software Support Centre] needed a powerful role from time to time, but the problem was it was allotted rather permanently rather than temporarily.' 14 June 2019, transcript of trial of *Bates v Post Office Ltd (No 6: Horizon Issues)* is published in Supplement, 18 *Digital Evidence and Electronic Signature Law Review* (2021).

[29] Superuser IDs; https://en.wikipedia.org/wiki/Superuser .

[30] Ian Henderson and Ron Warmington, 'Interim Report into alleged problems with the Horizon system', Second Sight Support Service Ltd, (2013), https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/pol_interim_report_signed.pdf .

Post Office, informed the Chair of the BEIS Select Committee in June 2020 that from 2014 the Post Officer ceased to act as a private prosecutor.

2013 In July and August, Simon Clarke, a barrister employed by solicitors working for the Post Office, provided a written opinion advising the Post Office that a witness from Fujitsu had failed to disclose information about known bugs in Horizon which could have helped the defence in criminal prosecutions. The purpose of this advice, according to the Post Office's solicitors,[31] was to notify the Post Office board and the corporation's insurers. Clarke's opinion was the subject of a board paper. The members of the ARCC therefore knew about the advice, and presumably that the risks it raised were sufficiently serious for the insurers to be notified. The obvious professional response of the ARCC directors would have been to inform the internal auditors and the risk managers who were monitored by Internal Audit. In a different written advice, dated August 2013, Clarke advised that he had been informed of attempts to avoid or, seemingly, circumvent disclosure obligations and that the word 'shredding' had been used to him in connection with documents. Clarke warned that this 'may well amount to a conspiracy to pervert the course of justice' [32]

Internal Audit should have close relations with Security and should certainly have been represented by an IT auditor in the conference calls about the Horizon problems or have requested minutes of these calls. If the Post Office Internal Audit had a competent IT audit function it would be remarkable if the auditors were unaware of the issues raised by Clarke. The implication is that the Post Office IT audit function was incompetent or non-existent. If this Clarke advice was hidden from Internal Audit, that raises concerns about the competence of the department. It would be surprising if alert and competent IT auditors were unaware of the issues raised by Simon Clarke.

Detica (a BAE Systems company) carried out a six-month investigation into fraud and non-compliance in the Post Office branch network.[33] The report was issued in October 2013. Detica's investigation had many of the features of a system audit and listed a series of problems with the technology supporting the Post Office's management of branches:

> 'Post Office systems are not fit for purpose in a modern retail and financial environment. Our primary concern here relates to difficulty in reconciling information from multiple transaction systems both in terms of timeliness, structure and access'.

[31] Letter from Peters & Peters to Aria Grace Law, 12 November 2020, in connection with *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, https://www.postofficehorizoninquiry.org.uk/sites/default/files/2021-11/Williams%20Inquiry%20Post%20Office%20Paul%20Marshall%20Submission%203%20November%202021R.pdf .
[32] *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, [81]-[89].
[33] Detica Net-Reveal. 'Fraud and Non-conformance in the Post Office; Challenges and Recommendations', 2013, https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/document_25_-_detica_netreveal_fraud_analysis_011013_1.pdf ; Detica Limited was renamed BAE Systems Applied Intelligence Limited in January 2014 .

Detica explained that Horizon's data were inconsistent with the data held by Galaxy, the Post Office's stock ordering system, which made it impossible to perform reconciliations between the systems. Detica also reported 'a fundamental issue with the process or controls in place around cash balancing'. This issue was so serious, and discrepancies so common, that branches which always balanced cash exactly were suspected of fraud.

The Detica investigation was performed at the same time as that of Second Sight and it was obviously relevant to the work of the forensic accountants. However, Second Sight confirmed to the author that their investigators were unaware of Detica's work and that the report was withheld from them. Second Sight also confirmed that during the investigation their investigators were not contacted by Post Office Internal Audit. It is extremely surprising that Internal Audit was so detached from such an important investigation.

2015 At a hearing in February 2015, BIS Select Committee members demanded to know why Second Sight was being denied full access to Post Office prosecution files they had requested.[34] According to Ian Henderson, the investigating forensic accountant (who was appearing before the Committee), the evidence that Second Sight was allowed to see was insufficient to support a charge of theft. Second Sight was then refused access to other files from late 2014 and in 2015.

Mr Henderson also clarified Second Sight's interim report, which had found no evidence of system wide, or systemic, errors at the software level. The Post Office had portrayed this as a finding that Horizon was free of errors. Mr Henderson pointed out that the finding related only to software causing system wide problems; there were local problems, and also problems with hardware, communications links, at the interfaces with other systems, and with the user experience. All of these could affect SPMs.

Second Sight was getting uncomfortably close to what eventually emerged in the subsequent litigation. In March 2015, the Post Office gave notice of termination of Second Sight's contract and they were directed to hand over or destroy all the material they had gathered, according to James Arbuthnot MP in a House of Commons question to the Prime Minister.[35]

Within about a month of the Select Committee hearing in February, the Post Office withdrew from the Second Sight review and from the mediation scheme for SPMs chaired by Sir Anthony Hooper (a retired judge of the Court of Appeal). Second Sight's final report was submitted to the Post Office in April 2015, with

[34] Business, Innovation and Skills Committee, Oral evidence: 'Post Office Mediation', HC 935, 3 February 2015. https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/business-innovation-and-skills-committee/post-office-mediation/oral/17926.html .

[35] Hansard, Prime Minister's Questions, Wednesday 11 March 2015, https://hansard.parliament.uk/Commons/2015-03-11/debates/15031163000022/engagements .

a copy retained by BEIS.[36] The report[37] details numerous bugs and features of Horizon. The report explained how an honest procedural error could generate a discrepancy that the Post Office would then assume to be fraudulent. The report also noted that the Post Office's power to force SPMs to repay any losses meant it did not always investigate discrepancies. The Second Sight final report included the statements that:

> '22.11 … for most of the past five years, substantial credits have been made to Post Office's Profit and Loss Account as a result of unreconciled balances held by Post Office in its Suspense Account.
>
> 22.12. It is, in our view, probable that some of those entries should have been re-credited to branches to offset losses previously charged.'

Second Sight therefore considered it 'probable' that unexplained discrepancies had been assigned to suspense accounts, and then taken by the Post Office as profit when the unexplained, and questionable, loss would already have been recovered from the SPMs. Not only should this have raised serious questions from internal auditors about Horizon, but it should also have caused them to scrutinize the way that discrepancies were investigated.

In August 2015 the BBC broadcast a Panorama documentary about the Horizon prosecutions.[38] The programme stated that the prosecution files in the case against Jo Hamilton in 2006 revealed that the investigators had found no evidence of theft. This was consistent with Ian Henderson's evidence to the Select Committee six months previously. Also, the Post Office had allegedly conceded that the most likely cause of the apparent losses was 'operational errors'.

Further, Charles McLachlan, an expert witness in the Horizon prosecution of Seema Misra[39] (whose conviction was quashed on appeal in 2021) said he had been told by a Post Office investigator that as a matter of policy the corporation would never consider a computer error to be the source of a discrepancy. The BBC also interviewed Richard Roll, a former contractor with Fujitsu, who confirmed that he had regularly amended branch data centrally in a way that the Post Office had insisted was impossible. This assertion carries particular force in the light of E&Y's findings about a lack of control over privileged user IDs.

At this point, in 2015, I will call a halt to the chain of evidence and warnings. In April 2015 the Criminal Courts Review Commission (CCRC) confirmed that it was starting to review the cases of SPMs convicted of theft and false

[36] Amanda Solloway MP, Parliamentary Under-Secretary (Department for BEIS), Parliamentary Questions, 29 September 2020 https://questions-statements.parliament.uk/written-questions/detail/2020-09-29/96797 .
[37] Ian Henderson and Ron Warmington. 'Initial Complaint Review and Mediation Scheme: Briefing Report Part Two'. Second Sight Support Service Ltd, 2015, https://www.jfsa.org.uk/uploads/5/4/3/1/54312921/document_34_-_second_sight_final_briefing_report_part_two_1.pdf .
[38] BBC Panorama, 'Trouble at Post Office', 17 August 2015.
[39] The transcript of the trial is published at 12 *Digital Evidence and Electronic Signature Law Review* (2015) Introduction, 44 – 55; Documents Supplement, https://journals.sas.ac.uk/deeslr/issue/view/328 .

accounting.[40] In November 2015 the JFSA announced that it was preparing Group Litigation against the Post Office.[41] After the relentless barrage of bad publicity and political concern at the highest level, the Post Office's board, and in particular the Audit, Risk and Compliance Committee (ARCC), which reports to the main board, should have been applying urgent pressure on their experts working within the Three Lines of Defence to help understand the risks that the corporation was facing.

The last line of defence was Internal Audit, which had the powers to act decisively, and should have seen the need to do so. Their responsibilities are not simply an internal matter that end when they report to the board. Internal auditors have a wider professional responsibility to oversee the whistleblowing process and, if necessary, to act as whistleblowers themselves.

Corporate governance and whistleblowing

The position of a whistleblower within the corporate governance structure is not obvious and it is worth explaining.[42] Whistleblowers are subject to protection from unfair treatment of dismissal, but only if they fall within certain categories:[43]

> 'You're protected if you're a worker, for example you're:
>
> an employee, such as a police officer, NHS employee, office worker, factory worker,
>
> a trainee, such as a student nurse,
>
> an agency worker,
>
> a member of a Limited Liability Partnership (LLP).'

This excludes SPMs from being officially designated, and therefore protected, whistleblowers. They are self-employed and sign a contract to provide a service to the Post Office.[44] It would nevertheless have been difficult for SPMs to act as whistleblowers in the Post Office's culture. If a problem manifested itself at their branch a Post Office investigation would start from an assumption that the SPM had made a mistake or acted dishonestly. The Horizon system was always assumed to be correct and the SPM would have had no credibility,

[40] Karl Flinders, 'Criminal Courts Review Commission set to review subpostmasters' claims of wrongful prosecution', Computer Weekly, 29 April 2015, https://www.computerweekly.com/news/4500245279/Criminal-Courts-Review-Commission-set-to-review-subpostmasters-claims-of-wrongful-prosecution .
[41] Justice for Subpostmasters Alliance. 'JFSA prepares for Group Litigation against Post Office', November 2015, https://www.jfsa.org.uk/november-2015.html .
[42] Public Interest Disclosure Act 1998; see also Whistleblowing for employees, https://www.gov.uk/whistleblowing ; 'Whistleblowing: Guidance for Employers and Code of Practice', Department for Business, Innovation and Skills (March 2015), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf .
[43] 'Whistleblowing for employees', https://www.gov.uk/whistleblowing .
[44] 'Post Office Network Transformation - Business, Innovation and Skills Committee - The future role of the subpostmaster', https://publications.parliament.uk/pa/cm201213/cmselect/cmbis/84/8408.htm .

Internal auditors have a clear responsibility to oversee the whistleblowing process, and the lack of whistleblowers draws attention to the failings of the Post Office's corporate governance. Internal auditors must either assure the board that there is an effective whistleblowing route, or the auditors must be prepared to act as whistleblowers themselves. It is the policy of the IIA that internal auditors must do one or the other.[45] If necessary, internal auditors should be prepared to report concerns externally, according to the IIA policy position paper on whistleblowing:

> 'If concerns are not taken seriously or overridden, an internal auditor may well face the prospect of considering whether to communicate the information outside the organisation, either by external whistleblowing to a regulator or other authority, or by public disclosure' if escalation to board level is ineffective.'

If internal auditors find themselves in this position, they should consult the IIA's Practice Advisory 'Communicating Sensitive Information Within and Outside the Chain of Command' issued in May 2010:[46]

> 'The decision to communicate outside the normal chain of command needs to be based on a well-informed opinion that the wrongdoing is supported by substantial, credible evidence and that a legal or regulatory imperative, or a professional or ethical obligation, requires further action.'

This Practice Advisory provides criteria that might justify external whistleblowing. The four criteria that are relevant to the Horizon case are as follows (set out on page 2):

- Criminal offences and other failures to comply with legal obligations.
- Acts that are considered miscarriages of justice.
- Acts that endanger the health, safety, or well-being of individuals.
- Activities that conceal or cover up any of the above activities.'

It would have been difficult and uncomfortable for Post Office internal auditors to fulfil this responsibility. But auditing is a well-paid profession. Receiving a good salary without living up to the associated responsibilities can be considered to be unprofessional. However, internal auditors are not the only people that are responsible. The ARCC, and ultimately BEIS, also failed in their duties to exercise responsible corporate governance.

Corporate governance – how it should not be done

I have listed the clear pattern of warning signs surrounding the Horizon system that unfolded over many years and explained how the Post Office's ARCC and Internal Audit had both the power and responsibility to act. What we know about their response is of relevance. It is impossible to provide detail, but it is self-evident that the response was wholly inadequate.

[45] Chartered Institute of Internal Auditors, 'Position paper: Internal audit and whistleblowing', (2013), https://www.iia.org.uk/resources/ethics-values-and-culture/whistleblowing/position-paper-internal-audit-and-whistleblowing/ .
[46] Chartered Institute of Internal Auditors, 'Practice Advisory 2440-2: Communicating Sensitive Information Within and Outside the Chain of Command', (2010), page 2. Not available online to non-members.

The formal reporting of risks in the Post Office's annual reports

It is possible to understand the Post Office's high-level reporting of corporate governance and risk by looking at the annual reports.[47] There has been a section on risk management in each of the reports since the Post Office split from Royal Mail in 2012. The risk management section has listed the principal and strategic risks facing the corporation and how they are mitigated. The risks that are mentioned are all worth addressing, but none of them are as grave, or as high profile as the risk to the Post Office's business that was presented by the Horizon system.

The Horizon system has never featured as an identifiable and *identified* risk in any annual report. It surfaced only indirectly in the 2019 report, but only as a litigation risk, which was (incorrectly) thought to be mitigated by contesting the litigation that took place. Even this risk had vanished in the 2020 report, the potential consequence stated in the 2019 report of 'legal findings and court orders which have an adverse impact on financial performance and/or reputation' had materialised. The Post Office had already had to admit that it could not afford to pay full compensation and that the government would have to support the Post Office financially.

The 2017 report mentioned the impending Horizon litigation, eighteen months after the High Court claim was issued. The report stated that the directors did not think that the outcome would have a 'material adverse outcome' on the group. By 2018 this had changed to 'an adverse outcome could be material' and the 2019 position is that 'an adverse outcome would be material'. The possibility of compensation being paid to the victims was mentioned for the first time only in 2019, four and a half years after the CCRC confirmed that it was reviewing Horizon prosecutions. However, that was not treated as a risk.

The treatment of the Horizon litigation over the series of three reports from 2017 to 2019 was inexcusably low profile and unrealistic. The implications were discussed in bland text, using standard paragraphs that are repeated word for word elsewhere in the reports. Despite all the warning signs over many years, the Horizon system was not identified as a technology risk in any of these annual reports. The Post Office treated the risk as an external threat arising through litigation and which they could manage by contesting the litigation. The real risk arose from the Horizon system and the way that the Post Office (and previously the Royal Mail) managed its own system. The risk, therefore, arose from the corporation's own decisions and actions. It was a fundamental error in risk analysis. If we are to take the annual reports seriously, the litigation risk appeared suddenly in 2019, and had dealt the corporation a potentially fatal blow by the time that the next annual report appeared. The real risk that the Horizon system presented had been visible for two decades.

This is the sort of dreadful scenario that effective risk managers and internal auditors should strive to avoid at all costs, even at the cost of their own jobs if they have any integrity. However, given the powers and responsibilities

[47] Post Office Limited annual report archive, https://web.archive.org/web/20211201221231/https:/corporate.postoffice.co.uk/secure-corporate/our-financials/post-office-annual-report/ .

vested in the ARCC, it should have been possible for the risk experts and auditors to carry out their jobs responsibly and without fear of retribution.

An ineffective IT audit function

The only sign I can find that the Horizon system itself was recognised as a risk came in a *Computer Weekly* story in 2016.[48] The Post Office chairman, Tim Parker, was quoted by *The SubPostmaster*, the official journal of the National Federation of Subpostmasters: 'I think that, for all its faults, Horizon is not a bad system at all and we'd incur considerable risks if we looked to replace it.'

Parker was speaking about the risk entailed in developing a massive, new, replacement system, but IT auditors, and indeed all experienced software developers, know that a large part of that risk arises from the old system. Such older systems are known as legacy systems and they are vital for corporations and governments across the world. They pose an awkward problem, a dilemma, for the IT world. Legacy systems evolve as they are extended and amended over the years. They become increasingly complex to the point that the results of any changes are unpredictable.[49] Worse, it is impossible to understand and describe in detail how they behave even before any changes are made, which makes their replacement extremely difficult. If one does not clearly understand what an old system is doing or how it works, any attempt to replace it is fraught with difficulty and will inevitably result in unexpected problems. The Wikipedia article on legacy systems depicts the dilemma.[50] The difficulty in understanding exactly what legacy systems do is presented both as a compelling reason for retaining them and a serious problem that must be confronted if one does retain them.

In 2018 I gave a keynote talk on this subject at the EuroSTAR Software Testing Conference. My paper 'Facing the dragons – dealing with complex unknowable systems' received the accolade of best conference paper and was published as an ebook,[51] and is also available in expanded form on my blog as 'The dragons of the unknown'.[52]

In such a confusing, unpredictable environment, audits of live systems acquire great importance. It is not enough to rely on pre-implementation testing, or on bug reports. Systems are adapted and evolve over the years. The testing of changes might be thorough, but these changes will introduce new pathways to failure that might not be immediately apparent. Old systems can be stable, run quite satisfactorily and perform a vital role for corporations at less than 100 per cent accuracy. Indeed, without exception, that is how complex systems run. Problems are most likely to arise at

[48] Karl Flinders, ''Considerable risk' if Post Office replaced Horizon system, says chairman'. *Computer Weekly*, 6 June 2016, https://www.computerweekly.com/news/450297820/Considerable-risk-if-Post-Office-replaced-Horizon-system-says-chairman .
[49] It is important to understand that large, modern IT systems behave like complex adaptive systems. The behaviour of the whole system cannot be understood by examining the behaviour of its components, which combine in unpredictable ways. As the system grows it evolves, with its behaviour changing in ways that are impossible to predict with certainty.
[50] 'Legacy system': Wikipedia. https://en.wikipedia.org/wiki/Legacy_system .
[51] J. Christie, 'Facing the dragons – dealing with complex unknowable systems', EuroSTAR (2018), https://huddle.eurostarsoftwaretesting.com/resources/functional-testing/facing-facing-dragons-dealing-complex-unknowable-systems/ .
[52] J. Christie, 'The dragons of the unknown', author's blog (2019), https://clarotesting.wordpress.com/the-dragons-of-the-unknown/ (see part 2 in particular: 'Crucial features of complex systems').

interfaces with other systems, and with other companies; organisational border zones often feature hazy responsibilities and unfounded assumptions about what other people are doing.

This mix of latent error, uncertainty about what systems are doing, and unpredictability about the effect of changes requires the sceptical, experienced, oversight that good IT auditors provide. They understand the difference between the system as imagined and the system as found, the difference between the idealised version imagined by higher management and the system designers, and the messy reality that users and support staff cope with.

Good IT auditors investigate whether and how systems fulfil their most important functions. They look for evidence, by interviewing the relevant people, analysing data and the system design, and conducting their own testing, that the system is reliably doing what it must do, and not doing what it must not do. They will then assess the implications if they find evidence that the system is failing, or if they cannot find evidence that the system is sufficiently reliable.

What they must not do is accept assurances that everything is fine or treat a lack of bug reports as evidence that the system is reliable. The absence of evidence of problems is most emphatically not evidence of a lack of problems.

The work of IT auditors falls mostly into two broad categories. They perform organisational level reviews, to establish whether the IT function is effectively managed and controlled. These were called installation audits where I worked. The term is not universal, but I will use it to describe all such high-level audits that focus on the management controls rather than the systems themselves.

The other type of audits entail detailed scrutiny of specific technical areas and systems. I shall call these system audits. Both installation and system audits are vital and inter-dependent. One cannot have confidence in system controls if wider management controls are missing or ineffective. There is little value in an elegant and impressive managerial regime if business critical systems are a poorly controlled mess at the technical level.

Installation audits can be performed relatively easily by experienced external auditors or consultants. The more detailed system audits require greater familiarity with the business context and the technology. It is difficult for an outsider to come in and perform these unless the client is prepared to incur the high costs of allowing external investigators sufficient time to immerse themselves in systems.

The Horizon system, with all its complexities and problems, required a detailed system audit, and this is what Second Sight were doing until they were dismissed in April 2015. It seems that the Post Office's Internal Audit team did not have enough suitable staff to perform such audits. When the Post Office separated from Royal Mail in 2012 it had only three people in its new Internal Audit team according to Malcolm Zack,[53] the first Head of Internal Audit. This was increased to five in 2013 and they had to cover all the normal Post Office activities as well as IT. Unsurprisingly the Post Office relied on external audit consultants.

[53] Malcolm Zack, Head of Internal Audit, Post Office, 2012-14, https://clarotesting.files.wordpress.com/2022/03/malcolm-zack-pol-head-of-internal-audit.jpg .

Therefore, at the crucial period in 2012 when the problems with the Horizon system were attracting increasing attention, the Post Office was clearly not equipped to conduct a detailed investigation of the system. Further, it seems that the corporation had not previously commissioned any audit of the system by external experts to provide assurance that the Horizon system was reliable. Surprisingly, evidence to support that claim comes from Paula Vennells, Chief Executive Officer of the Post Office from April 2012 to April 2019. Before being appointed CEO Mrs Vennells worked in a number of senior roles, including Managing Director.

Paula Vennells' defence of Horizon system audits

Paula Vennell's memory of alleged problems with the Horizon system differs from the timeline, based on contemporary press reports, set out earlier. This is what she told Darren Jones MP, Chair of the House of Commons BEIS Select Committee in June 2020:[54]

> '39. Turning to controls and security, these were the subject of audit by external consultants, including Post Office's auditors, Ernst & Young ('E&Y'). I wish to mention one such audit – in 2011 – because I have recently seen it suggested that the Post Office knew, or should have known, from the audit that there were serious problems with Horizon, of the kind which was revealed by the group litigation. I believe that I have a reasonably good recollection of the E&Y audit and its aftermath, and what has been reported in the press is not correct.
>
> 40. In their 2011 audit E&Y identified weaknesses in the control and security environment at Fujitsu's operation centres and recommended certain improvements but noted that the newly appointed CIO had the capability to drive the necessary changes. As a result, Post Office instructed E&Y going forward to conduct more in-depth audits using the SAS70 model, which I understood was the gold standard for IT audits. In 2012 and 2013 E&Y noted improvements to controls and security and made less significant recommendations for further improvements. Indeed, in their 2013 management letter, E&Y reported that focused management action had addressed many of the issues raised in previous years' audits, and that management was continuing to take steps to address challenges in the IT environment. Accordingly, while the 2011 audit raised concerns around controls, the outcome was ultimately positive.'

Mrs Vennells' statement is perhaps more revealing than she realised or intended. She conflates two issues that were related and does so in a misleading way. The two issues are the installation level controls and security on the one hand and the Horizon system problems on the other. The E&Y audits were at the installation level. The Horizon problems showed that a system audit was necessary, but this was not provided by SAS 70.

[54] Paula Vennells, Letter to Darren Jones MP, Chair of the Business, Energy and Industrial Strategy Select Committee, 24 June 2020, https://committees.parliament.uk/publications/1621/documents/15462/default/ .

SAS 70 and ISAE 3402 – installation level audits

The Statement on Auditing Standards Number 70 (SAS 70)[55] was a long-standing auditing standard emanating from the United States of America. SAS 70 was developed by the American Institute of Certified Public Accountants (AICPA), and widely recognized throughout the world. The standard was intended for conducting a service audit: that is, for auditing service providers (such as Fujitsu) so that outsiders could have confidence that systems being managed by these service providers could be relied upon for the production of financial statements by their clients.

SAS 70 was therefore relevant to the production of financial reports where the systems concerned might have a material effect on the accuracy of these reports. This was one of the reasons that SAS 70 was replaced in 2011. Corporations had found it valuable, but they were using it for purposes for which it was neither designed nor suitable. It was too narrowly focused on financial reports and could not be used credibly for audits covering security and privacy.[56]

In June 2011 the AICPA replaced SAS 70 with a new standard, the Statement on Standards for Attestation Engagements No. 16 (SSAE 16),[57] which was in turn replaced in 2017 by SSAE 18.[58] These standards mirrored and complied with the new International Standard on Assurance Engagements 3402 (ISAE 3402),[59] developed by the International Auditing and Assurance Standards Board (IAASB),[60] part of the International Federation of Accountants (IFAC).[61]

The E&Y management letter for the 2011 Post Office annual audit, mentioned above, and which was referred to obliquely by Paula Vennells, was issued in August 2011. Any service audits of the type to which Mrs Vennells was referring that arose from the E&Y letter should therefore have been ISAE 3402 audits.

The E&Y management letter mentions ISAE 3402 audits, noting that Fujitsu considered them 'excessively costly' and that 'the preference within POL at present is to focus on improving the existing audit process going forward'. E&Y recommended that the Post Office should keep the ISAE 3402 option 'under consideration'. During the Horizon Issues trial a Fujitsu witness, William Membury, provided a witness statement to that effect. He stated that E&Y conducted ISAE 3402 audits from the 2012/13 financial year, and that preparations began in 2011.[62] Mr Justice Fraser dismissed Mr Membury's evidence, observing that it was of little value and that it was 'a serious omission'

[55] Statement on Auditing Standards (SAS) No. 70, Service Organizations, https://web.archive.org/web/20210812084125/http://sas70.com:80/sas70_overview.html .
[56] Tommie W. Singleton, 'Understanding the New SOC Reports', ISACA Journal 2011, https://www.isaca.org/resources/isaca-journal/past-issues/2011/understanding-the-new-soc-reports .
[57] SSAE 16 Overview: https://www.ssae-16.com/ssae-16/the-ssae16-auditing-standard/ .
[58] SSAE 18: https://www.ssae-16.com/ssae-18-an-update-to-ssae-16-coming-2017/ .
[59] 'What is ISAE 3402?', https://isae3402.co.uk/isae-3402 .
[60] International Auditing and Assurance Standards Board, 'The IAASB sets high-quality international standards for auditing, assurance, and quality control that strengthen public confidence in the global profession', https://www.iaasb.org/ .
[61] International Federation of Accountants (IFAC) https://www.ifac.org/ .
[62] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), [500]-[507].

that he failed to mention the 2011 E&Y management letter that, according to Mrs Vennells, prompted the service audits.

It is unnecessary to spend too long discussing the appropriateness of SAS 70 because Paula Vennells' claim that Fujitsu's operation was audited effectively using the 'gold standard' SAS 70 model was misleading. SAS 70 may have been a well-respected model in its day, but it was obsolete by the time that E&Y issued the management letter. Not only that, but it was an installation audit. Such an audit is necessary, but not sufficient to establish whether a system is adequately controlled. E&Y's SAS 70, or ISAE 3402, audits would not have answered the questions and concerns about the Horizon system. They could have revealed problems with the managerial controls, such as the ineffective controls over privileged IDs, but they could not have demonstrated that the system was robust and adequately controlled.

Performing system audits

The System and Organization Controls approach to system audits

As noted, an IT installation can be well run, but its individual systems can be poorly controlled. However, it is impossible for the systems to be adequately controlled if the installation is poorly managed and controlled; a secure system cannot be built on weak foundations. If there are serious concerns about the reliability of a system, it is necessary to perform audits at both the installation and also at the system level.

The correct system audit model for Horizon would have been an ISAE 3000 audit and would have produced a System and Organization Controls (SOC) report. The SOC reports were defined by the AICPA[63] and have three levels, SOC-1, SOC-2 and SOC-3.

SOC-1 is the direct replacement for SAS 70. It is a widely recognised and the main way of complying with ISAE 3402 and SSAE 18, which are directed at the management controls that affect the financial data produced by an IT installation. SOC-1 reports come in two types. Type 1 offers an opinion on the controls in place at a point in time. Type 2 assesses whether the controls have been effective over a specific period.

The relevant model for a system audit in the era of SAS 70 would have been a SysTrust audit,[64] which was meant to provide assurance about particular systems. SysTrust was replaced, at the same time as SAS 70, by the AICPA's Trust Services Criteria (TSC).[65] These were designed to comply with ISAE 3000, the International Standard on Assurance Engagements. SOC-2 and SOC-3 audit reports are internationally recognised as a means of compliance.

[63] AICPA 'System and Organization Controls: SOC Suite of Services', https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html .
[64] '09. What is SysTrust? What is the difference between a SAS 70 and a SysTrust audit?', https://clarotesting.files.wordpress.com/2022/03/sas-70-faqs.pdf .
[65] AICPA '2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy', https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf .

SOC-2 and SOC-3 reports deal with the audit of individual systems. The two reports cover the same ground, but SOC-3 conveys the important information that matters most to outsiders unfamiliar with the systems. This is not like SOC-2, which considers the detail that matters to system experts. As with SOC-1, SOC-2 has two types of audit. Type 1 assesses whether appropriate controls have been designed. Type 2 assesses whether they are working effectively in the systems.

Both SOC-2 and SOC-3 audits are organized around the five TSC categories: (i) security, (ii) availability, (iii) processing integrity, (iv) confidentiality, and (v) privacy. Each of these has a number of criteria that well controlled systems must meet. The TSC and their criteria may have been formally defined little more than a decade ago, but they are not idealised, theoretical standards imposed on practitioners. They are essentially a codified form of long-established good practice and are strikingly similar to the way IT auditors were working long before 2011.

Lessons from the history of IT auditing

In the 1990s, when I worked as an internal IT auditor at one of the UK's largest insurance companies, our system audits were consistent with the TSC. We normally dealt with security, availability, confidentiality and privacy as part of installation level audits (i.e. SOC-1 equivalents) and would consider these categories only when the processing affected them. Our primary concern in these audits was processing integrity. According to the AICPA's '2017 Trust Services Criteria' (page 6, cited earlier), the processing integrity category:

> 'refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.'

This covers the approach that we would take as internal IT auditors. 'Validity' was not a separate criterion in our work; it was covered by accuracy and authorization. This remains the case; many practical applications of the TSC use only four criteria. Validity is incorporated into the other criteria.

The long-established credentials of the TSC are confirmed by an article in the January 1980 edition of the *Managerial Finance Journal*. Hart J. Will, a Canadian accounting and auditing professor wrote an article, 'Internal Auditing of Modern Information Systems (MIS)'[66] in which he argued that:

> 'Internal controls comprise all efforts to assure the accuracy, completeness, privacy, security, timeliness, truth, validity, and value of all formal information processing in organisations.
>
> External controls of MIS are the application of internal and external auditing functions and procedures—according to the Law of Requisite Variety or according to generally accepted auditing standards—to ensure that all control standards imposed on an organisation in a society or culture are met.'

[66] Hart J. Will, 'Internal Auditing of Modern Information Systems', Managerial Finance, Vol. 5 No. 2, pp. 171-187, January 1980. https://www.emerald.com/insight/content/doi/10.1108/eb013445/full/html .

Will's reference to Ashby's Law of Requisite Variety is intriguing. Ashby's Law is also known as The First Law of Cybernetics:[67]

> 'The complexity of a control system must be equal to or greater than the complexity of the system it controls.'

Stafford Beer explained it thus:[68] 'In order to regulate a system we have to absorb its variety.'

A stable system needs as much variety in the control mechanisms as there is in the system itself. This does not mean as much variety as the external reality that the system is attempting to manage – a thermostat is just on or off, it does not directly control the temperature, just whether the heating is on or off. The significance of Ashby's Law is explained in the abstract to Will's article:

> 'Modern information systems (MIS) have increased the variety of information systems which have been and can be designed to such an extent that auditors must finally recognise the Law of Requisite Variety.
>
> The auditability of MIS is a double-edged proposition since the variety of the MIS must be matched by auditors if they want to be recognised as control agents. Thus, either MIS variety must be reduced to match the audit variety achievable or the audit variety must be increased to match the existing MIS variety. In other words, an intelligent interface is needed between auditors and MIS. Auditors require a language and a communication channel to evaluate the internal controls of the MIS as well as the information generated by the MIS.'

IT auditors are part of the control mechanism for complex corporate IT systems. If they are to do the job effectively, they have to be able to probe systems and evaluate the internal controls in sufficient depth, as well as the effectiveness of the external controls provided by auditing standards and processes. If they wish to remain credible and relevant they cannot remain in the easy, comfort zone of working with and assessing only the external controls. Taking such an approach is, as Will warned, to assume that the variety in the IT systems is as simple as their approach. By the end of the 1980s the internal audit department of the insurance company where I worked had absorbed that lesson.

The recommended guidance for IT auditors provided by the IIA recognises the need for auditors to assess both the installation level controls and also the controls within individual systems. This is made very clear in the IIA's Global Technology Audit Guide (GTAG) 8: Auditing Application Controls.[69] The language used throughout the guide is essentially the same as that used in the TSC and Will's article; the processing has to be complete, accurate, authorized, and executed in an acceptable time period.

---

[67] John Naughton, '2017; What scientific term or concept ought to be more widely known? Ashby's Law of Requisite Variety', https://www.edge.org/response-detail/27150 .

[68] Stafford Beer, 'Designing Freedom', Massey Lectures, Thirteenth Series 1973, Toronto, Canadian Broadcasting Corporation, 1974, p. 21.

[69] Institute of Internal Auditors, 'Global Technology Audit Guide (GTAG) 8: Auditing Application Controls', (2007).

A formal SOC audit can be performed only by auditors accredited by the AICPA. However, good internal auditors can work to at least the standard required, and their greater familiarity with the business and local technology makes it easier for them to probe and interpret the detail than it would be for external auditors. External auditors must assess the internal controls of a corporation, of which internal audit is part. They can choose to rely on internal audit reports if they judge them to be reliable. In practice this mix of external and internal skill and experience is necessary in order to provide an acceptable level of assurance that systems are properly controlled. It seems that the Post Office was largely dependent on outside expertise.

An effective IT audit team has to be capable of assessing the internal controls of the systems. This has been standard professional practice for several decades. There is little sign that the Post Office's internal auditors were capable of working at this level. If they had done so they would surely have uncovered Horizon's flaws.

Mrs Vennells will no doubt have taken advice before writing to the BEIS committee. It should be stressed that the only IT audit she could cite was SAS 70 – that was both an obsolete and also an inappropriate model and standard. If there had been an appropriate system audit of the Horizon system, surely she would have stated this.

How financial systems can be audited responsibly

The professional standards of the IIA are principles-based.[70] They set out the requirements for professional conduct, along with interpretation to guide practitioners and criteria against which their performance can be assessed. I will describe how the internal audit department where I worked would audit financial systems in a way that would have complied with these standards. Being principles based these standards can be complied with in different ways. I provide only an example of how this may be done responsibly.

When as IT auditors we were assigned to audit a system, we would identify people who relied on the system to do their job and ask them to talk us through the business context of the system, sketching how it fitted into its environment. It was the interfaces where we always expecting things to go wrong. The scope of the audit was dictated by the diagrams (sketched diagrams of people's understanding of the systems, not verbal descriptions) drawn by the people who mattered, not formal system documentation.

We might have started with a blank sheet of paper on which we would ask users to draw their understanding of the system, but we were rigorous. We used a structured methods modelling technique called IDEF0[71] to make sense of what we were learning, and to communicate that understanding back to the auditees to confirm that we had made sense of the system and the business problems.

We constantly asked such questions as:

> How do you know that the system will do what we want?

[70] Institute of Internal Auditors, 'International Standards for the Professional Practice of Internal Auditing' (Revised: October 2016. Effective: January 2017), https://www.theiia.org/en/standards/what-are-the-standards/ .
[71] IDEF0 Function Modelling Method: https://web.archive.org/web/20220314103639/https:/www.idef.com/idefo-function_modeling_method/ .

How will you get the outcomes you need?

What must never happen?

How does the system prevent that?

What must always happen?

How does the system ensure that?

This is similar to the approach in safety critical concepts of 'always events' and 'never events' often adopted in medical safety circles. We were dealing with financial systems and we were most concerned with processing integrity. Processing integrity is concerned with whether processing is complete, accurate, authorized and timely. 'Complete, accurate, authorized and timely' was our auditor's refrain. I was repeatedly reminded of this when I was an inexperienced IT auditor.

Whether or not the system does what is required depends on the purpose of the system. Processing has to be sufficiently complete, accurate, timely, and subject to due authorization in order to satisfy that purpose. These criteria are all constrained by each other, and informed by the context, i.e. sufficiently accurate for the business objectives given the need to provide the information within an acceptable time after appropriate authorization. It was essential to understand the context. The current context in which the audit was being carried out was crucial. There may be more than a single purpose for a system, with different interested parties, and purposes can change and evolve over time.

It was always important to ask questions to help us identify the controls that would give us the right outcomes and prevent the unwanted ones, such as: 'Show me how you know that the system will stop users stealing money, or if any money is stolen, ensure the right person can be held accountable?' It was expected that there should be evidence that the system would behave the way it was supposed to. Mere assertions were not good enough. Given what is known about the Horizon system, had auditors asked such searching and detailed questions, it is hard to imagine that they would have received credible or satisfactory answers.

Once we had a good idea of the processes, the outputs, the key risks to the corporation, and the controls that were needed, we would test the system to see if we could force it to do what it should not do or prevent it doing what it was required to do. The approach to testing was to adopt the mindset of a dishonest or irresponsible user.

Ordinary users would be viewed in action. Our interviews, observations, and our own testing told us far more about the system and how it was being used than the formal system documentation could. It also told us more than we could learn from the developers who looked after the systems. They would often be taken by surprise by discoveries of how users were in fact working with their systems.

IT auditors would work closely with the other internal auditors. The company had a team of branch auditors who performed annual audits at the company's 100 or so offices. The IT auditors would assess the systems and the branch auditors would use these audited systems as a basis for their work.

In their submission to the February 2015 Parliamentary select committee hearing that was concerned with the Post Office review by Second Sight and the mediation scheme, the solicitors Howe & Co identified a crucial failing in the Post Office's approach to internal auditing. That failure was that there was no vouching of transactions, that is to say, there was no objective authentication of what they found against a reliable oracle. The Horizon system simply presented figures that were accepted at face value:[72]

> 'Instead of performing a real audit, POL's 'auditors' simply assume that the balances on Horizon are correct, compare them with those in the branch and prosecute the subpostmasters if the balances in the branch are less than those on Horizon. Hence, in reality no vouching of transactions whatsoever is undertaken by POL's 'auditors'.
>
> Using the term 'audit' to describe POL's intervention in the branches gives its actions a veneer of professionalism and depth of analysis which is in fact entirely absent. The lack of proper audits undermines the cases against the subpostmasters…'

The branch auditors where I worked were part of the internal audit department. In the Post Office they were not. This is clear in the LinkedIn entry for the Head of Internal Audit between 2012 and 2014 (see above), where he wrote that his Internal Audit department consisted of only three people. He states that branch auditors were in the second line of the Three Lines of Defence. They were therefore compliance staff, rather than internal auditors, who form the third line.

Ian Henderson of Second Sight offered an interesting insight into the Post Office's investigation of discrepancies when he gave evidence to the House of Commons Justice Committee in 2020.[73] He repeated the allegation that Charles McLachlan made on the BBC's Panorama programme in 2015:

> 'The investigations were usually extremely limited. Problems with Horizon were effectively off limits to investigators, who, as a matter of policy, were not allowed to consider Horizon as the cause of the reported shortfalls.
>
> The priority was finding evidence to support the prosecution case to the exclusion of all other possibilities. Both investigators and prosecutors routinely ignored their duty to pursue all reasonable lines of inquiry.'

[72] Written evidence submitted by Howe & Co Solicitors (POM 19), BIS Select Committee hearing on the Complaint Review and Mediation Scheme, 2015, https://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/business-innovation-and-skills-committee/post-office-mediation/written/17874.pdf .

[73] Justice Committee Oral evidence: Private prosecutions: safeguards, HC 497 Tuesday 7 July 2020, https://committees.parliament.uk/oralevidence/673/pdf/ .

This is in stark contrast to my own experience when conducting fraud investigations. We had to remain aware of the need to find out what had happened, and not simply look for evidence that supported our working hypothesis. We would always start with the original data, analysing the source files and searching for significant links and patterns. We were required to follow the trail of evidence all the way from the original data. Investigators had to remain alert to the possibility they might miss vital, alternative routes that could lead to a different conclusion. It is easy to assume too early that a suspect is guilty, and ignore anything inconsistent with that belief. Working on these investigations gave me great sympathy for the police carrying out detective work. If progress is to be made you cannot follow up everything, but it is necessary to be aware of the significance of the choices you do or do not make.

A major concern is what basis there was for the Post Office's auditors' and investigators' confidence in the accuracy of Horizon's figures. It seems certain that there was no reliable basis. Confidence was merely grounded in managerial assertion. That is not an acceptable basis for auditors, who require objective evidence. Difficult questions arise: did Internal Audit not know about this? Or did they know about the problem, but ignore it?

Three issues arising from the Horizon system

It will be useful to take a closer look at three significant and problematic topics in which IT auditors would take a keen interest. These topics are first, the importance of the 'business purpose', second 'implicit requirements', and third, the need for appropriate authorization.

The importance of the 'business purpose'

There is a phrase in the AICPA definition of processing integrity that requires close attention: 'Processing integrity addresses whether systems achieve the aim or purpose for which they exist'. What matters is not the purpose that might have been set out in the original development documents. What matters is the purpose that the system serves, what it is doing now, how it is being used now; the aim or purpose for which it exists. Stafford Beer adopted an aphorism[74] widely used in systems theory discussions: 'The purpose of a system is what it does.' Auditors must assess the system according to the purposes that they identify, not only those that are dictated to them by management.

Horizon is an interesting case of a system the purposes of which have evolved over time. Originally designed for the payment of government welfare benefits through Post Office branches, it was adapted to be the accounting system for these branches. Horizon might seem an extreme case, but it is hardly unique. Many IT systems survive for many decades. When I was a Y2K (concerning the century date change) test manager in the late 1990s, I was working with systems written when I was at primary school. These systems are adapted as the business changes and they become embedded in the technical infrastructure of a company. It can be surprisingly difficult to identify and define the crucial purposes for which they are required.

There were four different broad purposes of Horizon:

[74] 'POSIWID – the purpose of a system is what it does', Design4services, 2018: https://design4services.com/concepts/systems-thinking/posiwid/ .

(i) it provided data to the corporate accounts,

(ii) it allowed the Post Office to manage the accounts of individual branches,

(iii) it was the means by which the SPMs could manage their branches' finances and,

(iv) it served as a source of evidence in legal proceedings, whether criminal or civil.

The contrast between the purposes of corporate financial accounting and criminal investigation are of particular concern. These are drastically different purposes. Auditors and software testers would have found different problems and provided different audit and test reports depending on which purpose was subject to review.

It seems likely that the Horizon system was never adequately assessed for the purpose of fraud investigation – other than by Second Sight in their review, that was terminated by the Post Office in early 2015 shortly after the February 2015 select committee hearing. The Post Office wrongly seems to have assumed or believed that Horizon was fit for this purpose. It is striking that the only public defence of system audits at the Post Office was provided by Paula Vennells to the BEIS Select Committee Chair in June 2020. But she relied, inappropriately, on SAS 70, an installation level audit model designed to assess whether the installation's systems could produce reliable financial statements.

Even if Mrs Vennells had mentioned SysTrust, the systems level equivalent of SAS 70, or its replacement SOC-2, that would have been meaningless unless the auditors were instructed that a significant business purpose was to provide evidence that was sufficiently reliable to convict SPMs of fraud. A SysTrust or SOC-2 auditor might have found that Horizon was perfectly adequate for the production of the annual accounts, but hopelessly deficient as a source of criminal evidence. This is an issue that has, to date, received insufficient consideration, but it is an issue that should be obvious to competent IT auditors.

Not only was SAS 70 a high level, management controls, audit, but its focus on financial statements also meant that auditors would be worried only about problems that would materially affect the financial accounts. The Post Office's published accounts round figures to the nearest million. Seema Misra was jailed over an alleged shortfall of £74,000. For Janet Skinner it was £59,000. For Noel Thomas it was £48,000 and for Tracy Felstead it was £12,000. All four were imprisoned for losses that, even in total, would have been lost in mere rounding errors in the corporate accounts.

Assessing the Horizon system by its ability to produce evidence that would convict SPMs would not have produced a flattering verdict. The system was wholly inadequate for that purpose. It took a dreadful mix of corporate misconduct and exploitation of the legal presumption of the reliability of computer evidence to secure those hundreds of convictions – a presumption that ironically was introduced at about the same time as the Horizon system was rolled-out (from 2000).[75]

[75] For which see Chapter 5 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London,

The scandal was possible only because the Post Office covered up the flaws of the system and nobody spoke out. In *Hamilton v Post Office Ltd*[76] that Court of Appeal confirmed [at 55] that judges in the criminal cases had not ordered appropriate disclosure of evidence by the Post Office. Such disclosure would have undermined the Post Office's reliance on the presumption of reliability. The result was that many innocent people were convicted. Competent and diligent internal auditors would have exposed both the inadequacy of the system for its business purposes and also the cover up. They would have realised that these resulted in miscarriages of justice, which as the IIA Practice Advisory (cited above) makes clear, could justify external whistleblowing.

The 'processing integrity' criterion of accuracy is particularly troublesome. Experience of IT audit, software development and testing shows that different systems in different contexts demanded different approaches to accuracy. For financial analysis and modelling it was counterproductive to try to achieve 100 per cent accuracy. It would be too difficult and time consuming. This pursuit might introduce such complexity and fragility to the system that it would fail to produce anything worthwhile, certainly in the timescales required. A system that is 98 per cent accurate might be good enough to provide valuable answers to management and quickly enough for them to exploit them. Even 95 per cent could be good enough in some cases.

In deeply complex systems it might not even be possible to say what 100 per cent accuracy means, or to know whether it has been achieved. Systems can run quite satisfactorily with levels of inaccuracy that are considered acceptable in context. With complex financial applications that are summarising and modelling vast quantities of data, an honest and constructive answer to the question 'is the application correct?' would be some variant on 'what do you mean by correct?', or 'I don't know – it depends'. It might be possible to say the application is definitely not correct, if it is producing obvious nonsense. But the real difficulty is distinguishing between the seriously inaccurate, but plausible, and the acceptably inaccurate that is good enough to be useful. Often accuracy is a question of experienced judgment rather than arithmetic.

In other contexts, when dealing with customer's financial transactions, it is necessary to have a far higher level of accuracy. Losing a customer's data or making serious miscalculations with the price charged to a customer should be unacceptable, even if only a tiny fraction of the customers are affected. If 100 per cent accuracy is impossible, and it usually is, then IT auditors would expect to see some safeguards or controls to detect and handle exceptions rather than a naïve assumption that the processing is always correct.

Perhaps the most famous quote in software testing is from Gerald Weinberg, who shaped so much of that community's thinking: 'Quality is value to some person'.[77] When forming an opinion about the quality of a system, it is necessary to be clear about its role and what the main users need. The Horizon system was performing very

2021), published on paper and open source at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures .

[76] [2021] EWCA Crim 577, [55].

[77] See an interesting blog post by Mr Weinburg dated 23 September 2012 on this topic at http://secretsofconsulting.blogspot.com/2012/09/agile-and-definition-of-quality.html .

different roles for different people, which is hardly unusual, but in that case, it led to persistent confusion about the quality of the system.

Worse, the Post Office actively spread and encouraged confusion about quality. It appears that Horizon allowed the Post Office to manage its corporate accounts to an acceptable level of accuracy for the purposes of the whole organisation. However, for the other purposes, and especially for the SPMs, the level of quality was abysmal.

The problem of implicit requirements

When a live system is audited, the specifications of the requirements and design do not matter. In my experience these are not even considered because:

1. Specifications were a partial and flawed picture of what was required at the time that the system was built. In particular, some of the most important requirements were so fundamental to the secure and reliable operation of the system that they might not have been specified explicitly. These implicit requirements were so obvious that it was taken for granted that the system would comply. They 'went without saying'.

2. The specifications were not necessarily relevant to the business risks and problems facing the company at the time of the audit – the core purposes of the system may even have changed since implementation.

3. The system's compliance, or failure to comply, with the specifications told us nothing useful about what the system was doing or should be doing (we genuinely did not care about compliance).

4. We never thought it was credible that the specifications would have been updated to reflect the changes made since the system was released.

5. We were interested in the actual behaviour of the people currently using the system, not what the analysts and designers had thought they would or should do.

6. A system audit was usually scheduled for a specific, limited length of time. It might take all or most of the available time simply to resolve the differences between different versions of the historic documents.

Looking through the specifications, accordingly, is a waste of time. The flows of data, the risks, and the controls, in which we were interested were those that mattered to the people who understood why the corporation needed the system at the time of the audit. In particular, new categories of users, or interested parties, might have needs that were not reflected in the original requirements. It was nevertheless possible for experienced and skilled auditors to infer from interviews what these new groups needed, and what vital implicit requirements must be met.

Implicit requirements are a particularly difficult problem when dealing with external suppliers, or the providers of an outsourcing service. There is a long history in software development of suppliers producing unrealistically low estimates, often based on a shallow, superficial understanding of the requirements, in order to secure the

business.[78] Customers subsequently have found the cost increasing as they made expensive change requests. Even if the supplier acts ethically, there is an ever-present danger of excessive optimism, with essential, complicating detail being ignored. In either case, vital requirements are often left unstated. Effective system auditing can reveal the problems that follow from this failure to make essential requirements explicit.

Second Sight's two reports raise important questions relating to the implicit requirements that apply to suspense accounts in any well-designed accounting system. The second report expressed concern that 'some of those unexplained losses (attributed to SPMs) could be represented by transactions subsequently taken to the credit of its P&L Account'.[79] This should have resulted in urgent investigation by the Post Office to establish what was happening.

An accounting system must incorporate the double entry principle. If any erroneous or inaccurate entries are created, then compensating entries must be created to keep the system in balance. The correct place for them is in a suspense account. When Horizon bugs created false deficits in branches there would therefore have been a corresponding entry in a system suspense account.

Suspense accounts are merely temporary receptacles for entries that require further investigation. ISACA (Information Systems Audit and Control Association, an international professional association focused on IT governance) defines them as follows:[80]

> 'A computer file used to maintain information (transactions, payments or other events) until the proper disposition of that information can be determined… Once the proper disposition of the item is determined, it should be removed from the suspense file and processed in accordance with the proper procedures for that particular transaction.'

Such investigation is a matter of priority. Failure to investigate, or resolve, these items should raise concerns about the processing integrity of a system. Writing off unexplained suspense entries to the Profit and Loss account is a last resort. If there is a consistent pattern of large amounts being written off, there must be doubts not only about the processing integrity of the system, but also about the competence of the accountants, the system experts, and also the management culture.

The design and management of Horizon's suspense accounts makes it difficult, perhaps impossible, to establish whether money in suspense accounts was wrongly taken from SPMs. This was confirmed by Post Office Chief Executive Nick Read at an oral evidence session of the BEIS Business Committee.[81] The Post Office did not have full records prior to 2005. Since that year the design of Horizon meant that much of the unexplained money 'went into a

[78] James Christie, 'It always takes longer! (part 2)', Section 'Honesty – it's an ethical issue', https://clarotesting.wordpress.com/2012/04/01/it-always-takes-longer-part-2/ .
[79] Ian Henderson & Ron Warmington. 'Initial Complaint Review and Mediation Scheme: Briefing Report Part Two'. Second Sight Support Service Ltd, 2015. [2.15-2.16].
[80] ISACA glossary of technical terms and acronyms, https://www.isaca.org/resources/glossary .
[81] Business, Energy and Industrial Strategy Committee, formal meeting (oral evidence session): 'Post Office and Horizon, 11 January 2022, https://committees.parliament.uk/event/6685/formal-meeting-oral-evidence-session/ .

general suspense account'; it is impossible to identify the source of this money or why it was assigned to a suspense account. That these problems had not been identified and addressed in more than two decades of Horizon's existence is deplorable.

The persistent presence of large, unexplained amounts in a system's suspense accounts should require close investigation by system auditors because it is relevant to all five criteria for the TSC processing integrity category in SOC-2 and SOC-3 audits: completeness, validity, accuracy, timeliness, and authorization. A competent system audit of Horizon would have established that the suspense account processing failed the criteria of completeness, accuracy and timeliness at least, and possibly also validity and authorization. Even if system auditors are not following the SOC audit model, it is basic good practice to investigate suspense accounts closely. Problems, or unexplained entries, are a well-known warning sign of fraud or poor internal controls.

The concerns raised by Second Sight about the use of suspense accounts should have been sufficient, on their own, to justify a detailed system audit. The possibility that the system was designed and built correctly according to the formal requirements is irrelevant. Insisting on the integrity of Horizon while ignoring Second Sight's warnings about the suspense accounts was an indefensible position. There was ample evidence to require action by Post Office Internal Audit.

Authorization and remote access

Authorization is a particularly interesting criterion in the context of Horizon. In my experience this was always one of our most pressing concerns as IT auditors, and one that was often not dealt with adequately in the formal requirements. Vital detail often fell into the category of implicit requirements.

Every non-trivial transaction, and certainly every financial transaction, had to be logged so that there was evidence of the user who was accountable. It is necessary, sometimes years after the event, for investigators to examine a transaction and identify those who had worked on it and approved it. This evidence was a vital building block for fraud investigations.

New systems required to be carefully integrated with the corporation's access controls framework so that named individuals would only have the exact access rights they required for their particular job. Access rights consist of permission to use certain functions and also a series of authority levels within each function, such as the ability to raise a substantial payment being restricted.

Systems should be assessed by how they perform the purposes for which they exist and are used. These would not necessarily have been reflected in the original requirements, and they might not even be explicitly stated by management. Systems must have appropriate authorization controls. No competent auditor would accept a lack of effective controls simply because they had never been explicitly specified.

A conspicuous and remarkable failure of Horizon – or rather the Post Office's and Fujitsu's management of the system and IT environment – is that it was both possible and routine for financial data to be changed without any

evidence being retained of the person responsible. It is deplorable that both the Post Office and Fujitsu failed to address this for at least four years after E&Y raised the problem in the management letter accompanying the 2011 accounts. The failure is especially glaring to an experienced IT auditor who would readily appreciate the significance and implications of E&Y's observations.[82]

In addition to audit experience, I spent three years as an information security manager for IBM, working with major customers on outsourced accounts. The E&Y 2011 management letter covers technical issues that would have fallen within my responsibilities at IBM; the control of privileged accesses.

IBM required us to enter discussions before the start of the outsourcing service about how customers required us to control the service, including access rights, and required us to reach agreement within a few months of the contract start date. If customers wanted us to apply a lower level of control than IBM recommended, which was rare, then we had to secure the customer's written confirmation together with the reasons for their requirements. We were required to produce an agreed plan to provide the required level of control and implement that as quickly as possible.

It is worth noting that the Post Office's insistence that it was impossible to amend branch data remotely could never be true for systems where the data is held centrally, as it was by Fujitsu. If it were true, it would be impossible to perform essential processes such as backup and recovery of data following a hardware failure or disaster. An important point about IT system management is that installations do not, and are not designed to, prevent remote access, but to ensure that they are done only by properly authorised staff at the correct times, with appropriate levels of control, logging and monitoring.

It is extraordinary that Fujitsu failed to address these issues 15 years after the start of the Post Office contract. They had not been fully resolved four years later. Failing to ensure an appropriate level of control was unprofessional and irresponsible, regardless of whether or not the customer had explicitly requested it.

It is not the responsibility of internal auditors to define or operate such processes and controls, but they should provide assurance that they are present and being operated effectively. The unaccountable, unrecorded remote access facility as described by Mr Justice Fraser in his Horizon Issues judgment, on its own and regardless of many other Post Office management failings he describes, is sufficient to show that the Post Office's internal audit function as part of Post Office corporate governance was neither competent nor effective.

The significance of Mr Justice Fraser's approach

Reading the judgment of the Horizon Issues case, and in particular appendix 1[83] with its discussion of the technical issues, I was struck by the way that the judge took an approach that was similar in some respects to an IT auditor conducting a SOC-2 audit. In the 313 pages of the judgment and 114 pages of the Technical Appendix there is no

[82] James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', Section 'Superusers going "off piste"', *Digital Evidence and Electronic Signature Law Review*, 17 (2020), 56-57.
[83] Technical Appendix to *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB).

mention of the traditional documents produced in software development; no requirements specification, no system specification. The phrase 'business requirements' appears only as a general term, not a specific document. The word 'specification' appears only once, as a plural, and it is part of a lengthy quote from a Post Office submission.

Mr Justice Fraser clearly had little interest in what the original systems analysts and designers thought the system should be doing. His concern was how the system behaved in the hands of its users, and whether the system met the needs of the people who mattered, in this case principally the Post Office's SPMs. His statement that a bug could be anything within a system that caused an unexpected result (see above) is significant. The Post Office's position from 1999 until the Horizon Issues trial was that if users were surprised by the behaviour of the Horizon system then it was they who made a mistake or failed to understand how the system worked.

Issue 14 (See Appendix – the Horizon Issues) is particularly interesting. This concerned the ability of the SPMs to use the system in the way they needed if there was a discrepancy or disputed transaction. Clearly, the Horizon system was hopelessly deficient in this respect, but the attitude of the Post Office and Fujitsu was that the system was working as designed, and that it was fulfilling the purposes of the Post Office. Mr Justice Fraser thought differently, as would any competent IT auditor had they properly evaluated and assessed the system.

The first six Horizon issues addressed by Mr Justice Fraser contain many themes that concern auditors. The first three issues are grouped under 'Accuracy and integrity of data'. The heading for the next three is 'Controls and measures for preventing/fixing bugs and developing the system'. These issues deal with accuracy, errors, reconciliations, controls, and risk. From an audit point of view the most striking word is integrity. Clearly Mr Justice Fraser was interested in the processing integrity of Horizon. His approach was very similar to that of an IT auditor.

Fraser J focused on the true purposes that he could discern for the Horizon system and was not distracted by the Post Office's more limited view. The judge also looked for and evaluated the controls that these purposes required, without consideration of what had been in the original specifications. This is the approach that good IT auditors have to take. If problems with an IT system result in a corporation being engaged in legal proceedings, the legal professionals will focus on the real behaviour of the system and the needs of its users. Focussing too narrowly on historic requirements and system documentation exposes the corporation to greater risk where there is a difference between specification and usage – and it is the job of internal auditors to help manage risk.

In taking the approach that he did, Mr Justice Fraser implicitly drew attention to the inadequacies of the Post Office's corporate governance, and of internal audit in particular.

The triumph of process over purpose

When considering internal audit, risk management and corporate governance, it is important to make a distinction between the processes in place, and the effectiveness of the management operating the processes. Effective risk managers and internal auditors must always take care to distinguish the process from the purpose of these processes, and scrutinise the underlying problems, risks, and threats. Better processes, and stricter regulation, will be ineffective without diligent corporate governance specialists.

The IIA fully understands this issue. Its guidance on auditing corporate governance[84] identifies two approaches to such audits. Process audits provide assurance that appropriate processes are in place and are being followed. Effectiveness audits provide a judgment on whether the governance functions are working effectively. Process audits can be performed by a typical audit team. Effectiveness audits require senior and highly experienced specialist auditors who can challenge the most senior management. Process audits are relatively easy. Effectiveness audits are far more difficult, and potentially painful for both sides. It is very tempting to focus on the easy option.

A major lesson from the collapse of the HBOS bank in 2008 was that there must be strong auditing of the effectiveness of corporate governance. There is no sign that this was present at the Post Office. The board's Audit, Risk and Compliance Committee (ARCC) must take responsibility for that. They ensured that the Three Lines of Defence was being followed – but not that it was effective.

This vital point was raised in the investigations following the collapse of HBOS. HBOS instituted the same credible Three Lines of Defence model as the Post Office. They had the right processes but failed to manage them effectively. HBOS were only superficially committed to the need for risk management, and lost sight of the risks that would ruin the bank. The reports by the Financial Conduct Authority (and Prudential Regulation Authority)[85] and the Parliamentary Commission on Banking Standards[86] were scathing, particularly so on the failure to recognise and manage risk. The Parliamentary Commission on Banking Standards offered this conclusion about HBOS corporate governance (at page 30):

> 'The corporate governance of HBOS at board level serves as a model for the future, but not in the way in which Lord Stevenson and other former Board members appear to see it. It represents a model of self-delusion, of the triumph of process over purpose.'

A major lesson from the HBOS collapse was that the effectiveness of corporate governance must itself be subjected to effective auditing. There is no sign that such auditing was present at the Post Office. The ARCC are responsible for that: the responsibility is theirs even if they do not wish to accept it. They oversaw the whole risk management framework, but they failed to act and identify the real risks facing the corporation, preferring instead to cover the easier, less significant risks. The Post Office board and BEIS itself learned nothing from the HBOS catastrophe.

The Post Office offers yet another painful 'model of self-delusion, of the triumph of process over purpose'.

[84] Chartered Institute of Internal Auditors, 'Auditing corporate governance', (2020). https://www.iia.org.uk/resources/corporate-governance/auditing-corporate-governance/?downloadPdf=true .
[85] 'The failure of HBOS plc (HBOS) - A report by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), (November 2015), https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/hbos-complete-report .
[86] Parliamentary Commission on Banking Standards. Fourth Report, ''An accident waiting to happen': The failure of HBOS', (March 2013), https://publications.parliament.uk/pa/jt201213/jtselect/jtpcbs/144/14402.htm .

Conclusion

The Post Office had more than enough evidence to convince them that there were serious flaws with the Horizon system. Much of this evidence was publicly visible, and the rest would have been available to any reasonably competent internal auditors – if they were prepared to demand access to the right information, which was their job. Yet the most senior executive and the board claim that they were unaware of these problems. If the corporate governance of the Post Office had been effective, it would have been clear to the board that they were likely to lose the Horizon litigation. It was certainly obvious that they should have lost. The only way that they could win was by trying to conceal damaging evidence. In attempting to cover up the problems that caused the scandal the Post Office took a huge risk, a reckless gamble, with the future of the corporation, or rather with the public money that would be required to bail them out if they lost the litigation.

A dispassionate and responsible analysis of the risks arising from Horizon and the litigation should have persuaded governance professionals, executives and directors that the corporation's decision, stated in the 2018 annual report,[87] to 'robustly defend' the subpostmasters' case because it supposedly 'lacked merit' was reckless at best. The failings of the Post Office's corporate governance go beyond accounting and IT. Modern internal auditors are expected to assess the culture of the organisation. This applies not only to its risk culture, that is to say, the shared values and attitudes towards risk that guide decision making, important though that is; it also applies to the wider corporate culture.

The July/August 2021 issue of the IIA's magazine *Audit and Risk*[88] carried an article that made it clear what is expected of internal auditors:

> 'To check whether the organisation is living up to its cultural expectations, internal audit should check "core" issues including "tone from the top", remuneration policies, performance management reviews, risk appetite policies and statements on company ethics, explains Liz Sandwith, chief professional practices adviser at the Chartered IIA. It is vital that internal audit also understands the key drivers behind culture, such as leadership, strategy, corporate responsibility, risk management and people management… The way in which internal audit reports findings on culture to the board is also important. "It is not internal audit's place to say that an organisation has the 'right' culture. An organisation's culture is set by the board: if executives want a certain kind of culture, that is their decision," Sandwith warns. "Internal audit can provide assurance around the message from the board, how it is communicated via policies and procedures, and whether employees adhere to these." '

[87] Post Office Limited Annual Report & Financial Statements 2017/18, https://web.archive.org/web/20211201221503/https:/corporate.postoffice.co.uk/media/46798/ara-201718-final-with-signatures.pdf .

[88] Neil Hodge, 'The human factor: auditing culture' *Audit & Risk Magazine*, Chartered Institute of Internal Auditors, July/August 2021, 37: https://www.iia.org.uk/audit-risk-magazine/Archive/audit-risk-magazines-2021/ .

That article may have been published in July 2021, but the IIA's approach to corporate culture is not new. In July 2013 the IIA's Committee on Internal Audit Guidance for Financial Services issued this guidance for internal auditors in the UK,[89] which became part of the Internal Audit Financial Services Code of Practice:

> 'Internal audit should include within its scope the risk and control culture of the organisation. This should include assessing whether the processes (e.g. appraisal and remuneration), actions (e.g. decision making), "tone at the top" and observed behaviours across the organisation are in line with the espoused values, ethics, risk appetite and policies of the organisation.'

Clearly, the Post Office was aware of its background as a public service and wanted to portray an image that it was something more than a normal commercial corporation; more socially aware, more responsible, more ethical. As the corporation proudly announces in the headline banner on the home page of its corporate website at the time of writing:[90] 'We're the Post Office and there's no one quite like us. At Post Office, we are a commercial business with a social purpose.' Each of its annual reports announces proudly the Post Office's commitment to the wellbeing, health and safety of its people. These stated good intentions amount to no more than pointless platitudes when compared to the reality faced by many SPMs. The dreadful experiences of this group of people went back long before the Post Office was separated from the Royal Mail, as is illustrated by this account of Tracy Felstead's experience:[91]

> 'In 2001 Tracy was a recent school-leaver … There was a Horizon computer record that showed a shortfall of £11,500 at the till she was working on at her Post Office branch. Under caution, interviewed by Post Office investigators at Peckham police station, she was asked: "can you demonstrate how you did not steal the money?"[92] Just reflect on that.
>
> She protested her innocence. She was prosecuted by the Post Office. There was no evidence she had ever physically taken any money. The Post Office and Fujitsu objected to the cost of providing the electronic evidence that had been requested by Tracy's expert witness. In the event the electronic evidence was not provided and her expert… was not called at her trial. On 26 April 2002 Tracy was convicted of theft. She was 19 years old. She refused to apologise when invited to do so by the trial judge, protesting she had done nothing wrong. She was immediately locked-up in a young offenders' institution.'

For many years the Post Office espoused an ethos of social responsibility, caring and ethical behaviour. Yet, its treatment of the SPMs was callous, possibly malicious. There was a consistent pattern of failure in the governance of the corporation that manifested itself in IT problems and, egregiously, in a response to these problems that by

[89] 'Effective Internal Audit in the Financial Services Sector; Recommendations from the Committee on Internal Audit Guidance for Financial Services', Chartered Institute of Internal Auditors, (2013), https://www.theiia.org/globalassets/documents/standards/leading-practices/effective-internal-audit-financial-global.pdf .
[90] Post Office Limited, Corporate website home page: https://web.archive.org/web/20220201162409/https:/corporate.postoffice.co.uk/ .
[91] Paul Marshall, 'Scandal at the Post Office – the Intersection of Law, Ethics and Politics', 19 *Digital Evidence and Electronic Signature Law Review* (2022) 12 – 28.
[92] *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, [185].

default assumed SPMs must be to blame and must be punished. The attitude of the investigators in the Felstead case, 20 years ago, was the opposite of the approach that a responsible IT audit function should have adopted towards the system under review. They asked Ms Felstead, 'can you demonstrate how you did not steal the money?'[93] A competent and responsible auditor should have asked a system expert 'can you demonstrate how you know whether money is stolen, and how you know exactly who was responsible?'

In the Post Office over a period of 20 years there has been a consistent pattern of mismanagement of IT, hopelessly naïve trust in the reliability of a hugely complex system, and in a willingness to sacrifice individuals in the interests of corporate convenience, despite the massive, latent risks to the future of the corporation that this behaviour was storing up. This pattern was present when the Post Office was part of the Royal Mail, and it persisted after it became a separate corporation.

There was a continuing cultural problem that was not the fault of any one person, although responsibility ultimately lies with the board. In such cases, it is incumbent on the corporate governance professionals to address, to attempt to remedy, and, where necessary, to expose the gulf between the corporation's stated ethos and the true organisational culture that guides the behaviour and conduct of individuals. It is an onerous role with heavy responsibility, but that is why they are well remunerated. That is why they are there.

The Post Office's corporate governance structure, its risk managers, its internal auditors, but above all, the board of directors and the ARCC all had sufficient evidence to warn them of the problems and risks. They chose to ignore or else cover up and conceal the evidence. They failed in their professional, statutory, and moral duties. The ARCC's terms of reference made it clear that internal audit should be conducted according to the professional standards and requirements of the IIA. They failed dismally.

In his submission to the BEIS Horizon inquiry Paul Scully MP, Minister for Small Business, Consumers & Corporate Responsibility, has stated:[94]

> 'Since the issues with Horizon surfaced, BEIS were reliant on Post Office Ltd's management to investigate issues with the Horizon system. We were assured that the system was robust and that the issues raised by the postmasters were being handled appropriately. BEIS pressed management on these issues, including instigating a review of the Post Office's handling of Horizon and its dealings with postmasters in 2015, and was given consistent advice from the company's management and its experts that appeared to verify these claims at the time. It is now clear that this was not the whole picture and, in hindsight, facts have come to light through the litigation that has revealed that advice received over that period was flawed.'

This response is unsatisfactory because it confuses and conflates the role of the internal auditors on the one hand and executive management on the other. The internal auditors, not Post Office management, should have provided

[93] *Hamilton v Post Office Ltd* [2021] EWCA Crim 577, [185].
[94] Paul Scully MP, Written evidence to the Business, Energy and Industrial Strategy Select Committee, March 2020, https://committees.parliament.uk/writtenevidence/1007/pdf/ .

assurance via the ARCC and UKGI to BEIS. Either BEIS was over-reliant on management's assertions, rather than asking the ARCC to utilise the internal auditors, or the auditors themselves failed to provide any effective challenge to executive management and provided an assurance that was unwarranted and unjustified, an assurance that had no basis in fact. As the submission notes (Annex A, paragraph 8):

> 'UKGI acts as the shareholder representative for BEIS. As part of this role UKGI hold a Non-Executive Director (NED) seat on the POL Board and sits on its Audit and Risk Committee and the Renumeration Committee… The NED's role is to challenge management, including the CEO, on financial and operating issues and the strategy to execute the company's objectives.'

Wherever the truth lies there was clearly a failure of corporate governance. The Post Office's governance framework, the Three Lines of Defence, was a credible, and suitable, model. It was not applied effectively. That failure was exacerbated by the inability of UKGI and BEIS, despite BEIS having a government representative on the board, to notice that governance was ineffective. The responsibility for this appalling scandal rests at the highest level. BEIS was represented on the board of directors and the ARCC which had access to sufficient information to enable ARCC and therefore the board to recognise the extent and nature of the problem. The full examination of corporate governance at the Post Office promised by the Williams inquiry makes necessary an examination of the role and conduct of both BEIS, and UKGI as the Post Office's owner and sole shareholder.

Where does responsibility lie? The available evidence suggest that it belongs on many desks – all at the most senior levels.

James Christie is a self-employed testing consultant with 35 years' IT experience, as a system developer and designer, business analyst, IT auditor, project manager, test manager and information security manager.

https://clarotesting.wordpress.com/about/

Appendix – the Horizon issues

This section quotes the Horizon issues verbatim from the judgment.[95]

Bugs, errors and defects in Horizon

Accuracy and integrity of data

(1) To what extent was it possible or likely for bugs, errors or defects to cause apparent or alleged discrepancies or shortfalls in branch accounts or transactions, or undermine the reliability of Horizon accurately to process and to record transactions?

(2) Did the Horizon IT system itself alert Subpostmasters of such bugs, errors and if so how?

(3) To what extent and in what respects is the Horizon System 'robust' and extremely unlikely to be the cause of shortfalls in branches?

Controls and measures for preventing/fixing bugs and developing the system

(4) To what extent has there been potential for errors in data recorded within Horizon to arise in data entry, transfer or processing of data?

(5) How, if at all, does the Horizon system compare transaction data recorded by Horizon against transaction data from sources outside of Horizon?

(6) To what extent did measures and/or controls that existed in Horizon prevent, detect, identify, report or reduce the following to an extremely low level of risk:

a) data entry errors;

b) data packet or system level errors (including data processing, effecting, and recording the same);

c) a failure to detect, correct and remedy software coding errors or bugs;

d) errors in the transmission, replication and storage of transaction record data; and

e) the data stored in the central data centre not being an accurate record of transactions entered on branch terminals.

[95] *Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB), [18].

Operation of Horizon

Remote Access

(7) Were Post Office and/or Fujitsu able to access transaction data recorded by Horizon remotely (i.e. not from within a branch)?

Availability of Information and Report Writing

(8) What transaction data and reporting functions were available through Horizon to Post Office for identifying the occurrence of alleged shortfalls and the causes of alleged shortfalls in branches, including whether they were caused by bugs, errors and/or defects in the Horizon system?

(9) At all material times, what transaction data and reporting functions (if any) were available through Horizon to Subpostmasters for:

a) identifying apparent or alleged discrepancies and shortfalls and/or the causes of the same; and

b) accessing and identifying transactions recorded on Horizon? .

Access to and/or Editing of Transactions and Branch Accounts

(10) Whether the Defendant and/or Fujitsu have had the ability/facility to

i) insert, inject, edit or delete transaction data or data in branch accounts;

ii) implement fixes in Horizon that had the potential to affect transaction data or data in branch accounts; or

iii) rebuild branch transaction data:

a. at all;

b. without the knowledge of the Subpostmasters in question; and

c. without the consent of the Subpostmaster in question.

(11) If they did, did the Horizon system have any permission controls upon the use of the above facility, and did the system maintain a log of such actions and such permission controls?

(12) If the Defendant and/or Fujitsu did have such ability, how often was that used, if at all?

(13) To what extent did use of any such facility have the potential to affect the reliability of the Branches' accounting positions?

Branch trading statements, making good and disputing shortfalls

(14) How (if at all) does the Horizon system and its functionality:

a. enable Subpostmasters to compare the stock and cash in branch against the stock and cash indicated on Horizon?

b. enable or require Subpostmasters to decide how to deal with, dispute, accept or make good, alleged discrepancy by

(i) providing his or her own personal funds or

(ii) settling centrally?

c. record and reflect the consequence of raising a dispute on an alleged discrepancy, on Horizon Branch account data and, in particular:

(i) does raising a dispute with the helpline cause a block to be placed on the value of an alleged shortfall; and

(ii) is that recorded on the Horizon system as a debt due to Post Office?

d. enable Subpostmasters to produce

(i) Cash Account before 2005 and

(ii) Branch Trading Statement after 2005?

e. enable or require Subpostmasters to continue to trade if they did not complete a Branch Trading Statement; and if so, on what basis and with what consequences on the Horizon system?

Transaction Corrections

(15) How did Horizon process and/or record Transaction Corrections?