Information Security Framework of Policies: Addressing the UK Post Office Horizon IT Scandal

Stanley Shaw

7th August 2025

Abstract

This report addresses the UK Post Office Horizon IT scandal, where software errors led to the wrongful prosecution of hundreds of subpostmasters between 1999 and 2015. Prepared for the Post Office executive board, it reviews IT and policy failures, proposes a framework of policies to prevent recurrence, and recommends a prioritised implementation order. Furthermore, it outlines measurable milestones and KPIs so the board can track progress and hold stakeholders accountable throughout the rollout. Assumptions are made due to limited public data, focusing on system reliability, data integrity, and governance.

Contents

1 Introduction

The UK Post Office scandal, spanning 1999 to 2015, saw the Horizon IT system, developed by Fujitsu, falsely report financial shortfalls, leading to over 700 wrongful prosecutions of subpostmasters for theft and fraud. This report, written from the perspective of a cyber security assurance officer, critically evaluates the IT and policy failures, proposes an Information Security Framework of Policies, and prioritises their implementation. It acknowledges limited public data availability and focuses on actionable recommendations for the executive board.

2 Horizon IT System Failures and Cyber Policy Review

2.1 Assumptions

Due to restricted access to internal documentation, this report is based on several reasonable assumptions. While it is likely that the Post Office had access to internal audit reports, software assurance records, and complaint logs, these materials were not publicly available for this analysis. As a result, the evaluation relies primarily on external sources such as judicial findings, expert testimony, and investigative reporting.

It is assumed that organisational and regulatory factors limited the pace of reform, making phased policy implementation more practical. Sub-postmaster complaints, although likely documented internally, were not available in full, so patterns of systemic failure could not be directly verified. It is further assumed that Horizon was deployed without adequate security audit or formal code review, as suggested by persistent defects and expert evidence. Lastly, the lack of publicly disclosed contractual safeguards indicates that vendor oversight may have been insufficient, particularly regarding remote access by Fujitsu engineers.

These assumptions are acknowledged to maintain transparency and directly inform the proposed policy framework and prioritisation.

2.2 UK Post Office Horizon IT Scandal Timeline

This timeline outlines key events that occurred during the post office scandal as well as judicial outcomes and further inquiry's.

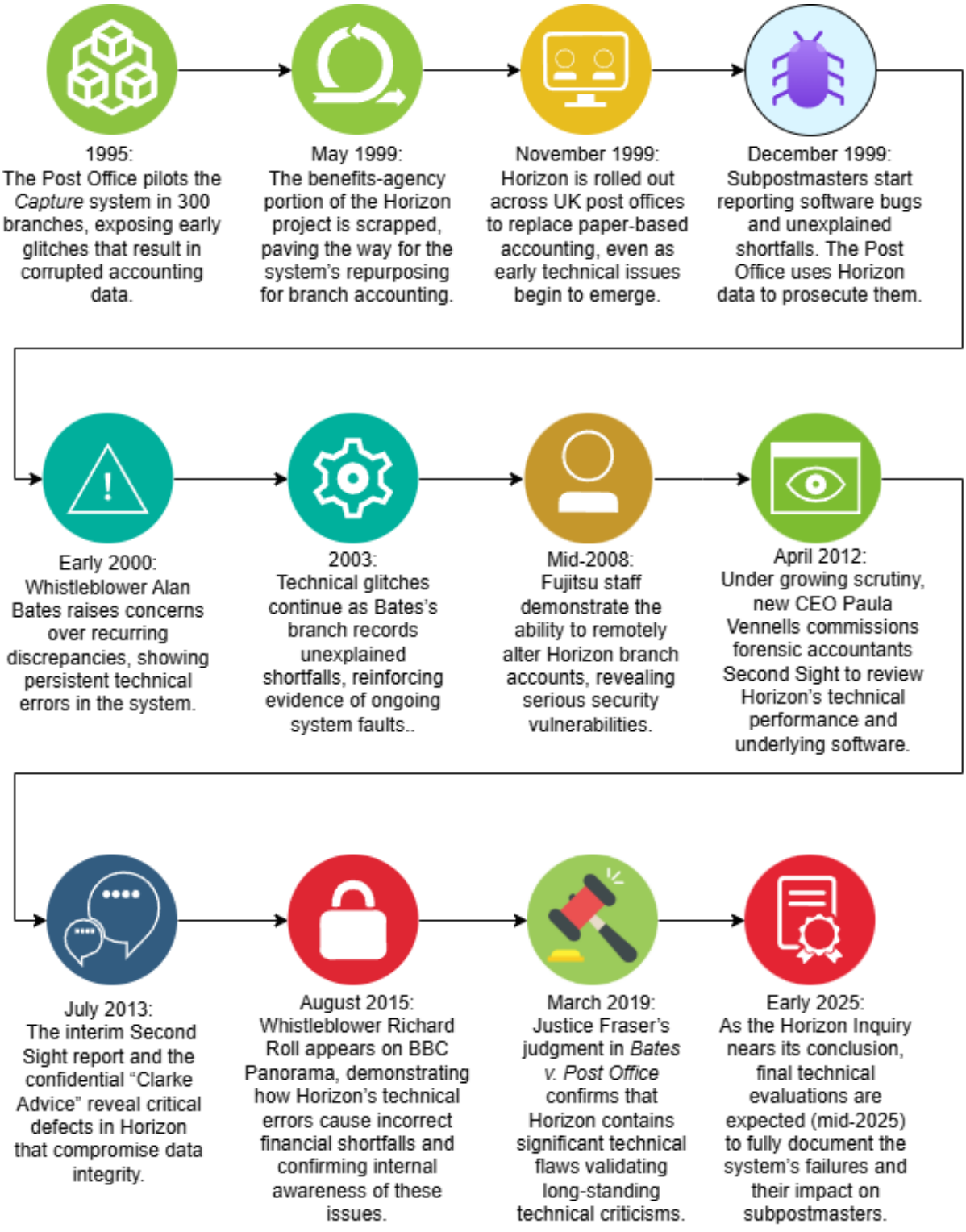

Figure 1: UK Post Office Scandal Timeline

2.3 Technical Failures in the Horizon System

Horizon was plagued by multiple software defects which compromised the reliability of branch accounts. In a 2019 High Court judgment, Justice Fraser stated that Horizon contained "bugs, errors, or defects" which led to unexplained discrepancies in sub-postmasters' financial records; the version deployed between 2000 and 2010 was deemed "not remotely robust" [High Court of Justice, 2019]. Key technical shortcomings included:

- **Software Bugs Causing False Accounting Entries**
  Critical bugs in transaction processing produced phantom losses. The Callendar Square bug duplicated withdrawals while the Dalmellington bug re-logged cancelled transactions, inflating branch deficits that went unflagged without automated reconciliation (see Figures 2, 3). Without robust real-time error detection and automated reconciliation safeguards, these anomalies went unnoticed, allowing phantom losses to accumulate and severely undermining the system's reliability [Hern, 2024].

- **Inadequate Error Handling and Auditing**
  Horizon rarely flagged or explained anomalies. During freezes or desynchronisations, no clear error messages or automatic reversals were provided. Actions like pressing "previous" or retrying could result in multiple recordings, leading to discrepancies wrongly blamed on user error or fraud.

- **Poor Software Quality Assurance**
  Horizon's development was severely flawed. Built by ICL/Fujitsu in the 1990s, it suffered from poor coding practices and insufficient testing. One developer noted "no standards were being followed," with specifications retrofitted for an individual process [Hern, 2024]. An IT expert later identified 29 bugs, 21 of which were later confirmed by Post Office experts indicating inadequate testing and patch management [High Court of Justice, 2019].

- **Lack of Robust System Design**
  As a financial platform, Horizon should have had a number of features including automatic reconciliation, duplicate detection, and audit trails. Instead, it relied on manual oversight, expecting sub-postmasters to detect and report errors. Furthermore, Fujitsu engineers were able to remotely alter branch data without the sub-postmasters' knowledge, and because back-end modifications were permitted as recently as 2023, the logs did not distinguish between routine and remote changes [Hern, 2024].

2.4 Governance and Assurance Failures

The Horizon scandal was not solely a technical failure—it also represented a breakdown in IT governance and risk assurance within the Post Office. A series of managerial oversights allowed technical issues to persist, while sub-postmasters' concerns went unaddressed.

- **Lack of Independent Oversight and Audit**
  No external audit was commissioned initially, and anomaly reports were dismissed. Only in 2012—after MP and sub-postmaster pressure—was Second Sight engaged; its 2013 interim report flagged serious bugs, but in early 2014 executives launched "Project Sparrow" to hinder the audit [Rawlinson, 2024].

- **Inadequate Internal Escalation of Issues**
  Horizon-related complaints were met with improvised solutions or dismissals rather than systematic investigation. Despite internal records showing similar discrepancies across branches, no process existed to aggregate or analyse them, marking a major governance lapse [High Court of Justice, 2019].

- **Failure to Disclose Known Issues**
  Executives withheld internal evidence of Horizon's defects and repeatedly asserted its reliability in legal proceedings. By ignoring warnings about legal obligations, they continued prosecutions on flawed data, severely undermining transparency and justice.

2.5 Cultural and Organisational Shortcomings

The technical and governance failures were compounded by a detrimental organisational culture. A pervasive "computer never lies" mindset stifled dissent and discouraged sub-postmasters from questioning Horizon's data. Employees were implicitly warned against challenging the system's reliability, which created an atmosphere of fear and silence. Internal critics were often labelled as adversaries, and sub-postmasters who raised concerns were met with hostility and punitive measures [Croft, 2024]. Furthermore, senior management appeared more focused on protecting the institution's reputation than addressing its systemic faults. Testimonies from former officials, including Sir Ed Davey [Davey, 2022] and Ron Warmington [Warmington, 2024], reveal a culture where accountability was lacking, and transparency was sacrificed in favour of institutional defence. This environment allowed the technical issues to persist unchallenged for many years.

3 Policy Analysis

To address Horizon's technical and governance failures, I developed an Information Security Framework of Policies grounded in contemporary cybersecurity literature and proven IT-governance practices. It aligns with ISO/IEC 27001 and NIST SP 800-53 controls [ISO, 2022a, NIST, 2020], and maps to ISO 27001 Annex A (see Figure 4), including controls such as A.14.2.1 for secure development and A.16.1.5 for incident response, and ensures structured, proactive risk treatment and mitigation [ISO, 2022a].

3.1 Risk Evaluation and Prioritisation

Before proposing individual policies, I first evaluated the top Horizon failures using a simple likelihood–impact matrix [ISO, 2022b]. Any risk scoring at or above *High* × *Major* exceeds my risk appetite and demands immediate treatment.

Table 1: Risk Evaluation Matrix for Horizon Failure Modes

Failure	**Likelihood**	**Impact**	**Above Risk Appetite?**
Duplicate transactions (Callendar Square)	High	Critical	Yes
Cancelled but logged transactions (Dalmellington)	Medium	Critical	Yes
Inadequate error handling and auditing	High	Major	Yes
Poor software quality assurance	High	Major	Yes
Lack of robust system design	Medium	Critical	Yes
Undisclosed remote data overrides	Medium	Critical	Yes
Lack of independent oversight and audit	High	Major	Yes
Inadequate internal escalation of issues	High	Major	Yes
Failure to disclose known issues	High	Critical	Yes
Cultural reluctance to challenge system reliability	High	Major	Yes

This matrix clarifies that every identified failure sits above my risk appetite, this guides me to prioritise policies targeting these critical areas. By quantifying likelihood and impact I can order my policy implementation based off the most impactful failures.

3.2 System Reliability and Quality Assurance

The system reliability and quality assurance policy mandates comprehensive testing including unit, integration, user acceptance (UAT), penetration, and regression tests. As well as scheduled updates to maintain resilience against emerging threats (see Table 1). Periodic independent audits provide unbiased evaluation of system integrity and compliance with industry standards.

By enforcing these measures, I directly mitigate the highest-risk failure modes identified in Table 1, including duplicate transactions (Callendar Square), cancelled-but-logged transactions (Dalmellington) and inadequate error handling, all of which were rated above my risk appetite. Rigorous testing uncovers such bugs before release, while external audits ensure that coding and patch management adhere to best practices.

Ensuring software is robust and free of critical vulnerabilities before deployment reduces the likelihood of faulty releases, safeguards operations and protects the organisation's reputation [ISO, 2022a, NIST, 2020]. Given the assumed absence of end-to-end audits prior to Horizon's rollout, this policy's external validation is essential to prevent flawed code from reaching production.

3.3 Data Validation and Integrity

This policy requires that system outputs be routinely cross verified against alternative data sources or manual checks, and that strict error reconciliation processes are followed to quickly identify and correct discrepancies. It directly addresses the high risk failure modes of cancelled but logged transactions (Dalmellington) and inadequate error handling, both of which exceed the risk appetite (see Table 1).

A robust whistleblowing framework allows employees and stakeholders to confidentially report any anomalies, thereby mitigating the failure to disclose known issues and enhancing transparency. Together, these measures ensure that critical decisions, such as prosecutions or financial adjustments, are based on accurate, validated data, preventing miscarriages of justice and preserving organisational integrity.

This policy aligns with ISO/IEC 27001 Annex A controls A.14.2.1 (Secure development policy) and A.14.2.9 (Testing in development and acceptance), embedding rigorous software assurance throughout the development lifecycle [ISO, 2022a, NIST, 2020].

3.4 Incident Response and Escalation

This policy requires a structured process for logging incidents, assigning investigation and escalation procedures, and defining clear roles for an incident response team. It ensures swift identification, containment and remediation of high-risk issues such as inadequate internal escalation and failure to disclose known faults (see Table 1). The policy mandates pausing critical actions, including legal proceedings, until a thorough investigation is complete. By institutionalising accountability and responsiveness, it prevents minor faults from becoming crises and protects against reputational, financial and legal harm. This policy aligns with ISO/IEC 27001 controls A.8.5.1 (Information backup), A.12.4.1 (Event logging) and A.16.1.5 (Incident response) and follows NIST SP 800-61 guidelines on incident handling [ISO, 2022a, NIST, 2012, 2020].

3.5 Governance and Accountability

Governance and accountability policies explicitly define oversight responsibilities, roles and accountabilities at various organisational levels. This includes detailed contractual agreements with IT service providers outlining service expectations, liability clauses and penalty provisions for non-compliance. Regular reviews and audits of contractor performance, compliance checks and governance effectiveness evaluations are mandated to prevent gaps in oversight. By institutionalising rigorous supervisory and accountability mechanisms, this policy addresses the lack of independent oversight that contributed to Horizon's failures (see Table 1). Its importance lies in ensuring transparency, enforcing responsibility and cultivating stakeholder trust, thereby strengthening organisational governance and effectiveness. This aligns with ISO/IEC 27001 controls A.5.1.1 (Policies for information security) and A.15.2.1 (Monitoring and review of supplier services), this policy ensures continuous supplier monitoring. In light of assumed deficiencies in contractor oversight, it targets systemic gaps in vendor accountability [ISO, 2022a, NIST, 2020].

3.6 Training and Awareness

A comprehensive training and awareness policy mandates periodic and systematic training programmes for all employees, particularly those directly interacting with critical information systems like subpostmasters. This includes sessions on correct system use, error identification, complaint procedures, cybersecurity best practices and incident reporting responsibilities. By cultivating informed vigilance and proactive reporting, this policy directly addresses high-risk failures such as cultural reluctance to challenge system reliability and inadequate internal escalation, significantly bolstering organisational resilience against technical and human errors (see Table 1).

Its importance is profound, as it ensures successful implementation and adherence to all other policies, thereby multiplying the effectiveness of the entire security and governance framework. This reflects ISO/IEC 27001 control A.7.2.2 (Information security awareness, education and training), which mandates ongoing staff capability building [ISO, 2022a, NIST, 2020]. As subpostmasters were discouraged from raising concerns, this policy ensures a shift in culture towards empowered reporting and transparency.

3.7 Policy Framework Overview and Mapping

After detailing the policies, it is clear that the proposed framework addresses both the technical and organisational failures identified in the Horizon IT system. Table 2 provides an overview of each policy's relevance and importance.

Table 2: Policy Framework Overview

Policy	**Relevance**	**Importance**
System Reliability and Quality Assurance	Addresses software-testing inadequacies and enforces independent verification	Critical for ensuring software robustness and reliability
Data Validation and Integrity	Implements cross-verification and whistle-blowing mechanisms for accurate system outputs	Vital for preventing incorrect legal and operational decisions
Incident Response and Escalation	Establishes structured incident reporting, investigation, and escalation procedures	Essential for rapidly resolving issues and mitigating impacts
Governance and Accountability	Defines clear oversight mechanisms and accountability for IT providers and internal staff	Crucial for transparency, responsibility, and stakeholder trust
Training and Awareness	Provides regular, systematic education on system use, security practices, and reporting mechanisms	Fundamental for supporting all policies and organisational security culture

To further illustrate the direct connection between the identified failures in the Horizon IT system and the proposed policies. Table 3 maps each failure to a specific policy along with its mitigation impact.

Table 3: Mapping of Horizon System Failures to Policies and Impacts

Identified Failure	**Proposed Policy**	**Mitigation Impact**
Software bugs causing false accounting entries	System Reliability and Quality Assurance	Comprehensive testing, independent audits, and stringent patch management reduce software errors and improve system robustness.
Inadequate error handling and auditing	Data Validation and Integrity	Automated error detection and data cross-verification prevent flawed data from influencing critical decisions.
Lack of independent oversight and audit	Governance and Accountability	Establishing an independent oversight committee ensures transparent monitoring and accountability of system performance.
Ineffective incident reporting and escalation procedures	Incident Response and Escalation	A structured incident-response plan enables swift detection, investigation, and resolution of issues, reducing operational impact.
Cultural reluctance to challenge system reliability	Training and Awareness	Regular training programmes and awareness campaigns foster a proactive security culture, empowering staff to identify and report anomalies.

Lessons from the SolarWinds and Fish Tank Casino breaches reinforce this framework's relevance. Both incidents reveal how inadequate software assurance and poor device governance enable lateral attacks. Policies addressing system reliability, supplier accountability, and staff training are not only vital for Horizon, but align with controls that mitigated these global cybersecurity failures [Kostopoulos, 2021, Tshisekedi and Al-Fuqaha, 2019].

4 Recommendations

4.1 Prioritised Implementation Order

Given the severity and impact of IT and policy failures highlighted by incidents such as the UK Post Office Horizon scandal, the following prioritised implementation of policy framework is recommended. Priorities have been established based on immediate risk mitigation, stakeholder impact, and long-term organisational security and operational improvement. The prioritisation of policies also draws from ISO 27005's risk treatment principles, which recommend addressing the highest residual risks first to stay within the defined risk appetite and maintain operational continuity [ISO, 2022b].

Table 4: Policy Implementation Priorities

Priority	**Policy**	**Rationale**
1	Data Validation and Integrity	Immediate implementation necessary to prevent decisions based on flawed or compromised data; critical to prevent wrongful prosecutions or faulty financial operations, ensuring trustworthiness of system outputs.
2	Incident Response and Escalation	Essential for promptly addressing complaints, mitigating further damage from incidents, and maintaining trust by demonstrating responsiveness and accountability.
3	System Reliability and Quality Assurance	Addresses the root causes of software inadequacies and prevents recurrence of systemic failures through comprehensive testing, quality assurance, and independent verification.
4	Governance and Accountability	Establishes necessary oversight and clear responsibilities for system governance, accountability, and transparency, crucial for maintaining long-term stakeholder confidence and ensuring compliance with legal and regulatory requirements.
5	Training and Awareness	Fundamental for embedding security consciousness and compliance within organisational culture, providing ongoing reinforcement of all other policy implementations, though with lower immediate urgency compared to direct risk mitigations.

4.2 Policy Remediations

The following specific remediations are recommended, each with clearly defined implementation timelines to address immediate vulnerabilities and establish long-term operational security:

Policy	Timeline	Recommendation
Data Validation and Integrity	Immediate – 3 Months	Deploy automated verification tools integrated within existing systems to perform cross-checks and real-time validation. Introduce routine audits and establish robust whistleblowing channels to rapidly identify discrepancies and potential fraud or inaccuracies.
Incident Response and Escalation	Immediate – 6 Months	Create and deploy a structured incident response plan that includes a 24/7 dedicated support hotline. Develop clear escalation pathways, response protocols, and designate responsible personnel to ensure timely and appropriate incident handling.
System Reliability and Quality Assurance	6 Months – 1 Year	Commission an independent comprehensive audit of existing software systems to identify and document existing vulnerabilities or testing inadequacies. Implement regular software update cycles and mandatory third-party verification processes to continually validate system reliability and functionality.
Governance and Accountability	6 Months – 9 Months	Formulate and establish an oversight committee comprising internal stakeholders and external independent experts. Clearly define accountability structures within updated supplier contracts and internal guidelines, ensuring that all software and IT infrastructure providers adhere to explicitly stated security and performance benchmarks.
Training and Awareness	1 Year Onwards	Initiate and sustain annual mandatory training programmes designed to build comprehensive security awareness across all organisational levels. Programmes should include practical training on system use, compliance requirements, security protocols, and reporting procedures, ensuring long-term effectiveness of policy adherence.

4.3 Implementation Milestones and KPIs

A granular overview of each policy's implementation plan—with assigned ownership, KPIs, and measurable targets that enable transparent tracking and Board-level oversight—appears in Table 5. Grounded in ISO/IEC 27001 Annex A control requirements and ISO/IEC 27005 risk-treatment principles, and aligned with NIST SP 800-53 guidance on continuous monitoring and performance metrics, this approach is mapped to the relevant standards in Figure 4, thereby supporting a structured, auditable governance process [ISO, 2022a,b, NIST, 2020].

Table 5: Policy Implementation Milestones and Expanded KPI Definitions

Policy	**KPI Definition**	**Owner**	**Target**
Data Validation and Integrity	Percentage of transaction anomalies automatically identified and flagged by the system (automated matches vs. total anomalies detected)	Head of IT Risk	$\geq 95\%$ detection rate within 3 months
Incident Response and Escalation	Average elapsed time from incident alert to initiation of containment actions (measured in hours)	Incident Response Lead	Detect in <1h, contain in <4h by month 6
System Reliability and Quality Assurance	Ratio of critical software defects found per thousand lines of code during each test cycle	QA Manager	Zero critical bugs in quarterly audit
Governance and Accountability	Proportion of contracted suppliers meeting all defined security service-level agreements in their quarterly reviews	COO	100% compliance by month 9
Training and Awareness	Share of employees completing the full security training curriculum and passing the post-training assessment	HR & Security Lead	100% annually

Policy rollout assumes sufficient technical capacity and organisational buy-in; feasibility factors such as cost, training load, and integration with existing processes will require further assessment during implementation planning.

5 Conclusion

The Horizon scandal highlights the dangers of relying on unverified digital systems without sufficient policy safeguards. This report presents a targeted framework addressing core failures in testing, data integrity, escalation, oversight, and awareness. If implemented in the prioritised order, these measures can rebuild trust, enforce accountability, and ensure future technological deployments are both secure and just. Beyond preventing technical failures, the framework promotes a proactive organisational culture, embeds transparency at all levels, and aligns with international standards to foster resilience. Ultimately, it provides a blueprint for ethical, secure, and evidence-based information system governance across complex public sector environments.

6 Appendix

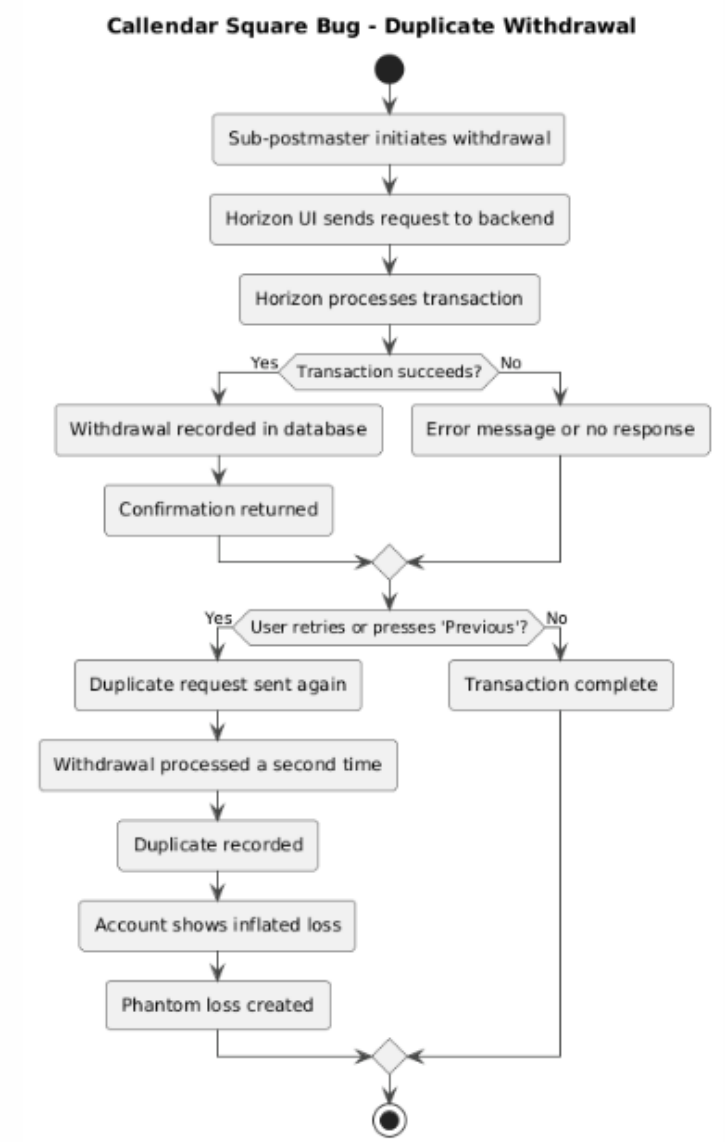

Figure 2: Callendar Square bug diagram

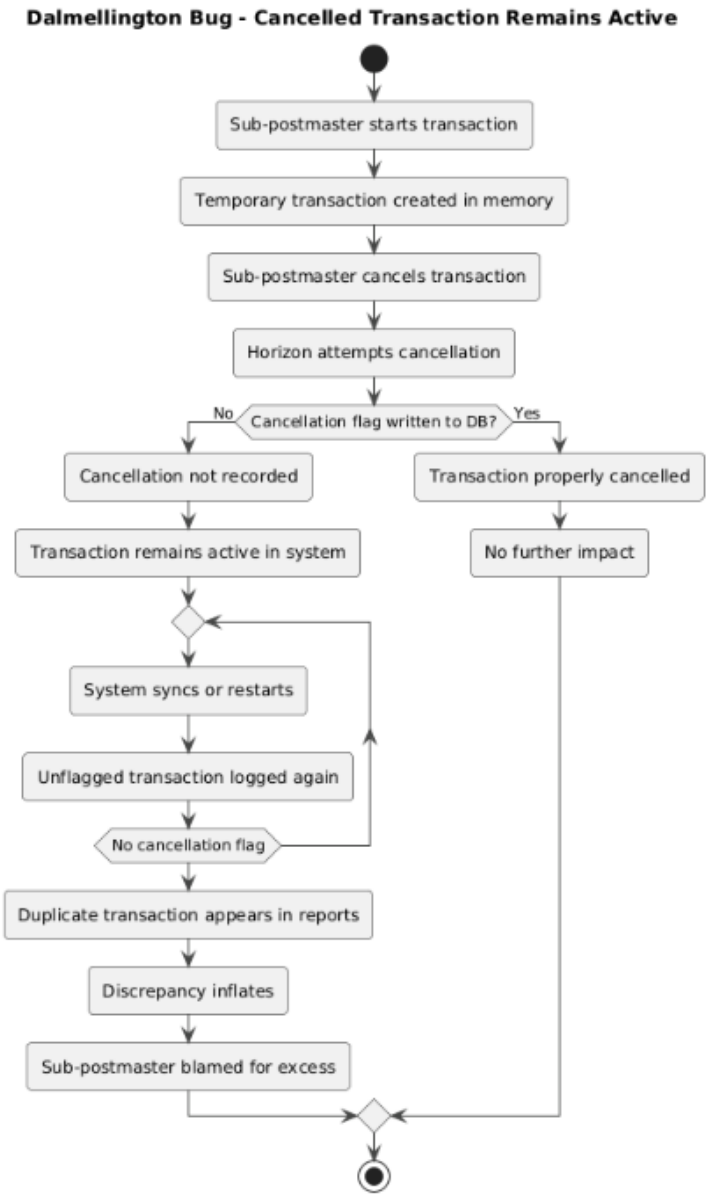

Figure 3: Dalmellington bug diagram

Policy	**Mapped ISO/IEC 27001 Controls**	**Related NIST Controls / Frameworks**
System Reliability and Quality Assurance	A.14.2.1 – Secure development policy A.14.2.9 – Testing in development and acceptance	NIST SP 800-53: SA-11 (Developer Testing and Evaluation) SA-12 (Supply Chain Protection)
Data Validation and Integrity	A.8.5.1 – Information backup A.12.4.1 – Event logging A.10.1.1 – Cryptographic controls	NIST SP 800-53: AU-6 (Audit Review, Analysis, and Reporting) SI-7 (Software, Firmware, and Information Integrity)
Incident Response and Escalation	A.16.1.1 – Responsibilities and procedures A.16.1.5 – Response to information security incidents	NIST SP 800-61: Incident Handling Guide NIST SP 800-53: IR-4 (Incident Handling)
Governance and Accountability	A.5.1.1 – Policies for information security A.15.2.1 – Monitoring and review of supplier services	NIST SP 800-53: PM-9 (Risk Management Strategy) CA-7 (Continuous Monitoring)
Training and Awareness	A.7.2.2 – Information security awareness, education and training	NIST SP 800-53: AT-2 (Security Awareness Training)

Figure 4: Mapping of Proposed Policies to ISO/IEC 27001 and NIST Standards

References

Jane Croft. Second Sight draft report on Horizon cases, 2024. Highlights the adversarial approach towards sub-postmasters and internal investigations.

Sir Ed Davey. Testimony of Sir Ed Davey, 2022. Testified regarding non-disclosure of Horizon bugs during his tenure.

Alex Hern. How the post office's horizon system failed: a technical breakdown. *The Guardian*, January 2024. Describes the "Callendar Square" and "Dalmellington" bugs and technical failures.

High Court of Justice. Judgment (No. 6) Horizon Issues, 2019. Cited in Mark Halper, *Communications of the ACM*, Jan. 2025.

ISO. *ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*. ISO, Geneva, 2022a.

ISO. *ISO/IEC 27005:2022 - Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks*. ISO, Geneva, 2022b.

George Kostopoulos. Lessons from the solarwinds hack: A new era of cybersecurity threats. *Journal of Cybersecurity and Privacy*, 1(1):45–54, 2021. doi: 10.3390/jcp1010004. URL `https://www.mdpi.com/2624-800X/1/1/4`.

NIST. Computer Security Incident Handling Guide. Technical Report NIST Special Publication 800-61 Revision 2, U.S. Department of Commerce, Gaithersburg, MD, 2012. Available at: `https://doi.org/10.6028/NIST.SP.800-61r2`.

NIST. Security and Privacy Controls for Information Systems and Organizations. Technical Report NIST Special Publication 800-53 Revision 5, U.S. Department of Commerce, Gaithersburg, MD, 2020. Available at: `https://doi.org/10.6028/NIST.SP.800-53r5`.

Kevin Rawlinson. Project Sparrow minutes and Post Office's strategy, 2024. Reporting on the Post Office's efforts to limit independent audit by Second Sight.

Lydie Tshisekedi and Ala Al-Fuqaha. Securing the internet of things: A case study of the fish tank hack. In *Proceedings of the International Conference on Internet of Things Security*, pages 92–97. IEEE, 2019. doi: 10.1109/ICIoTS.2019.00019.

Ron Warmington. Ron Warmington testimony to the Horizon Inquiry, 2024. Describes management's overly optimistic summary of Horizon issues.