Building an Effective Charity Internal Controls Framework:

A Practical Guide



www.wda.ie

CONTENTS

Executive Summary & Roadmap 3

2. Governance & RACI Accountability Framework 6

3. Step-by-Step Guide to Building A Control Universe 8

4. Policy Register Governance & Digital Staff Attestation 11

5. Risk Register Integration & Objective Residual Scoring 13

6. Performance Monitoring & Board Dashboard 15

7. Statutory Audit Alignment 17

8. Fraud Prevention, Cybercrime & Management Override Safeguards 19

9. Internal Audit Function 20

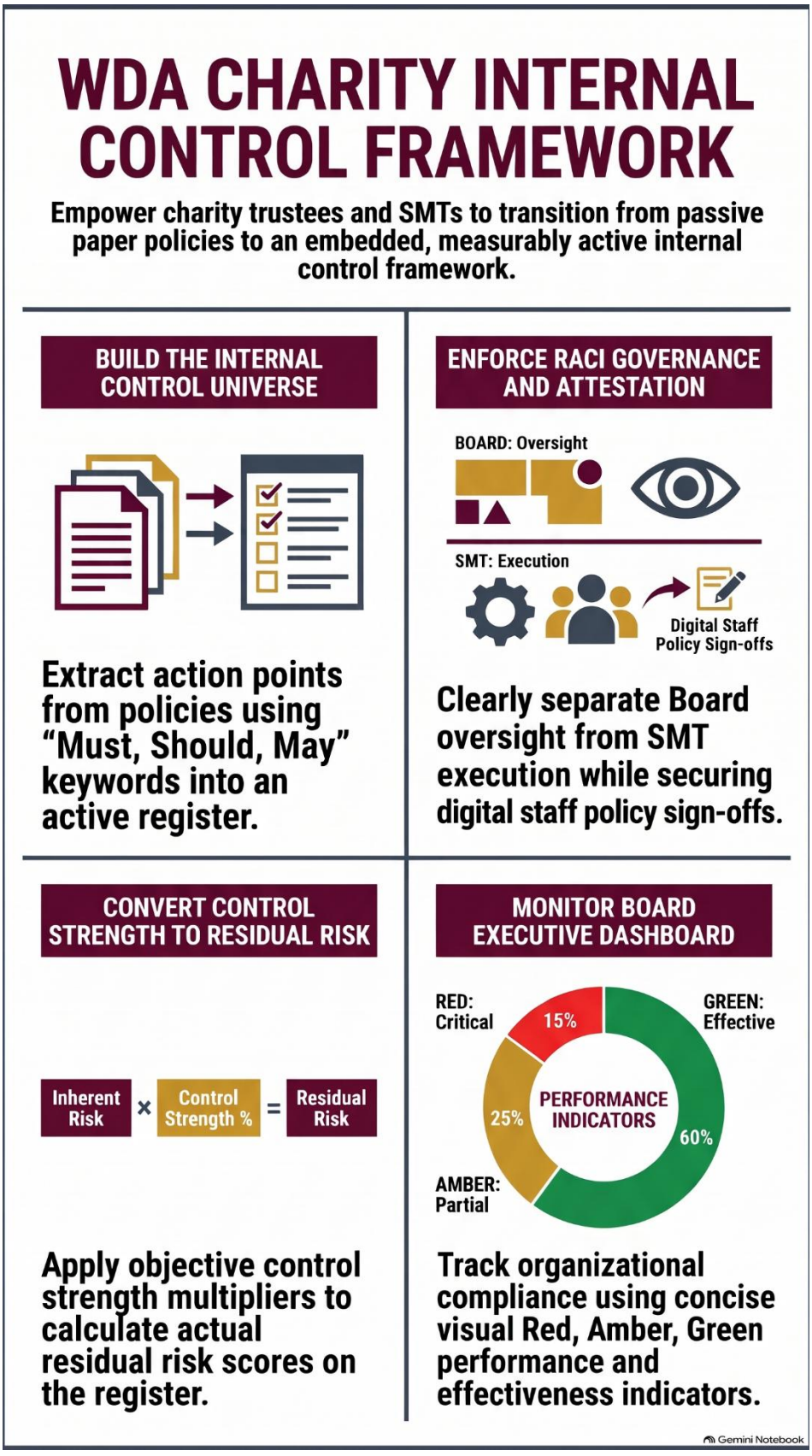
10. Phased 12-Month Implementation Roadmap 21

11. Common Sector Pitfalls 22

12. Strategic Recommendations 23

13.0 About WDA 24

EXECUTIVE SUMMARY & ROADMAP



1. Executive Summary & Governance Context

There is a prevalent and well-documented systemic weakness across the Charity and Not-For-Profit (NFP) sector in Ireland: a fundamental failure to demonstrate that internal controls are fully embedded and operationally active throughout the organization. While most charities possess comprehensive, director-approved written policies and procedures—covering financial management, fundraising, safeguarding, risk management, and human resources—there exists a 'Governance Gap' between policy approval and operational execution.

In practice, charity boards routinely approve policy documents during annual general meetings or board sessions, but subsequently receive zero systematic documentation or exception reporting confirming whether staff and Senior Management Teams (SMT) actually execute the underlying control procedures on a daily, weekly, or monthly basis. Policies remain static PDF files stored on shared drives or lever-arch folders creating a false sense of security among trustees until a financial misstatement, cyber incident, fraud event, or regulatory audit intervention occurs.

📌 THE INTERNAL CONTROL UNIVERSE PARADIGM

The core purpose of this handbook is to guide Charity Trustees and Senior Management Teams in bridging the Policy-Execution Gap. By deconstructing 20 – 40+ approved policy documents into an 'Internal Control Universe' (ICU), assigning clear RACI accountabilities, requiring digital staff attestations, linking control performance to risk register residual scoring, and generating board-level exception dashboards, charities transform passive compliance into real, verifiable operational assurance.

1.1 Legal and Regulatory Obligations for Irish Charity Trustees

Trustees of Irish charities operate under a stringent matrix of statutory and fiduciary duties. Incorporating internal control mechanisms is not merely best practice; it is a legal requirement governed by multiple statutory authorities:

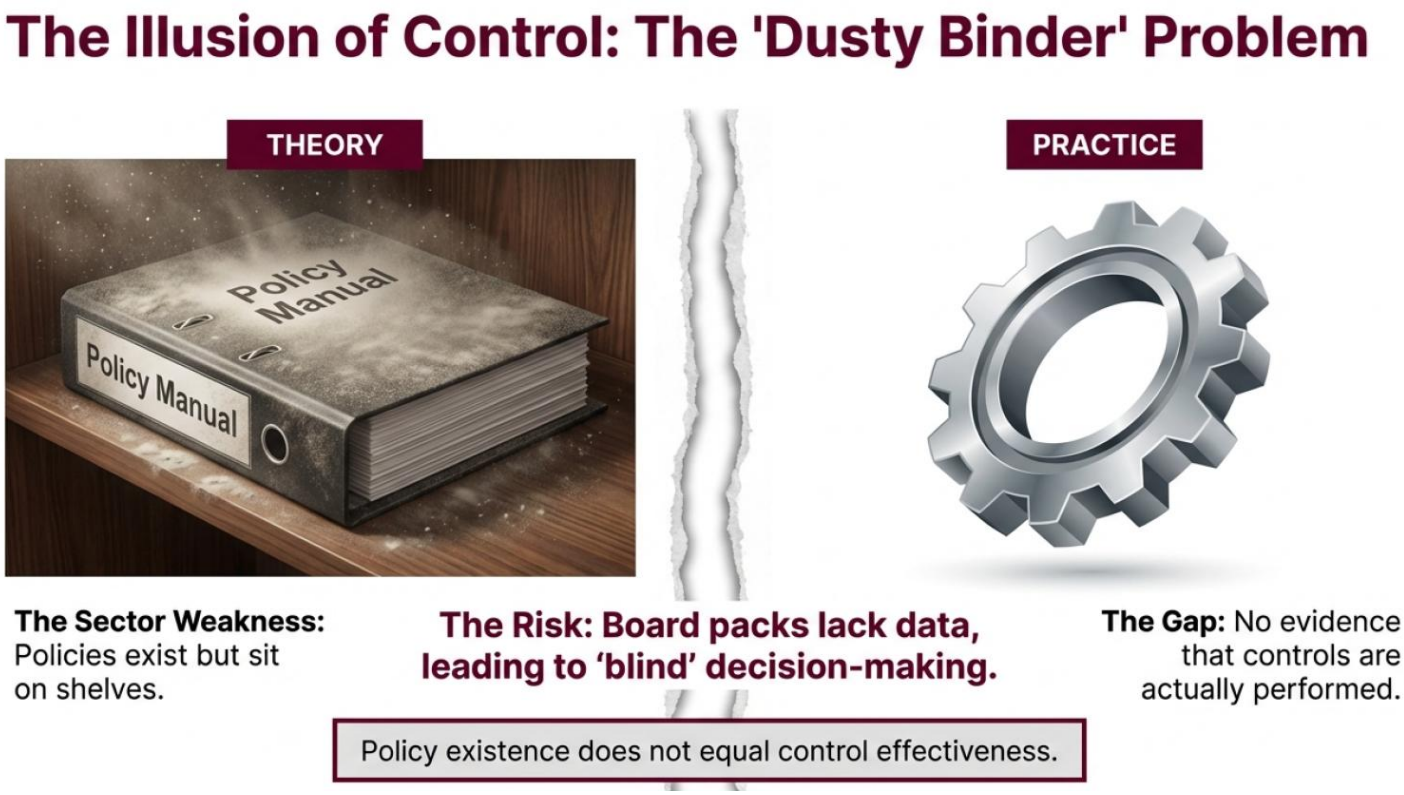
- **Charities Act 2009:** — Establishes statutory requirements under Sections 47–52 for charities to maintain proper books of account, submit audited annual returns, and operate under the oversight of the Charities Regulatory Authority (CRA). Under Section 47, trustees are legally responsible for ensuring that financial statements give a true and fair view of the charity's state of affairs.
- **CRA Internal Financial Controls Guidelines (2017):** — Explicitly mandates that charity trustees must implement robust internal financial controls to safeguard assets, prevent fraud or error, maintain complete accounting records, and protect organizational reputation. The CRA guidelines cover five mandatory operational domains: Income, Expenditure, Banking, Assets, and Financial Monitoring.
- **Charities Governance Code:** — Sets out six overarching governance principles. Principle 4 ('Exercising Control') mandates that trustees must regularly monitor financial performance, manage risk through an active risk register, ensure proper operational controls, and complete an annual Compliance Record Form under a 'comply or explain' framework.

- **Companies Act 2014 & ODCE Guidelines:** — Applies directly to Charities Limited by Guarantee (CLGs). Sections 281–285 impose strict statutory duties on company directors to maintain adequate accounting records that explain transactions, disclose financial position with reasonable accuracy, and enable financial statements to be audited efficiently. Failure to comply constitutes a criminal offense.

- **Charities SORP & FRS 102:** — Mandates application of FRS 102 accounting principles, enforcing strict fund accounting rules that segregate Restricted, Unrestricted, and Endowment funds. Internal controls must ensure restricted funds are spent strictly in accordance with donor mandates.

1.2 Board Governance vs. SMT Operational Accountability

A primary cause of internal control failure in non-profit organizations is the confusion between Board Oversight and Executive Management. Trustees are non-executive volunteers who cannot—and should not—manage daily operations. However, trustees remain legally accountable for organizational oversight. To resolve this tension, an Internal Control Framework creates a structured mechanism where SMT implements and documents controls, while the Board and Audit & Risk Committee (ARC) systematically review control performance metrics and exception reports.



2. GOVERNANCE & RACI ACCOUNTABILITY FRAMEWORK

To eliminate ambiguity regarding who executes, approves, and monitors control activities, charities must embed a formal RACI Framework (Responsible, Accountable, Consulted, Informed) across all internal control and governance activities.

2.1 Definitional Breakdown of RACI Roles

- **Responsible (R):** The operational staff member or manager who performs the control activity (e.g., executing dual-signatory bank approvals, performing monthly bank reconciliations, checking fixed asset registers).
- **Accountable (A):** The senior leader or trustee body with ultimate decision-making authority and ownership of the control outcome (e.g., CEO/CFO for operational execution; Board of Trustees for overall control system adequacy).
- **Consulted (C):** Key advisory bodies or subject matter experts consulted during control design or policy review (e.g., Audit & Risk Committee, legal advisors, external audit consultants).
- **Informed (I):** Stakeholders provided with periodic status updates, summary performance dashboards, or exception reports (e.g., Full Board of Trustees, Regulatory Bodies, Donors).

Lifecycle Stage	Board / Trustees	Audit & Risk Committee	Senior Management (SMT)	Control Owners	Internal/External Audit
Design & Document Policy	Accountable	Consulted	Responsible	Informed	Informed
Implement & Execute Control	Informed	Informed	Accountable	Responsible	Informed
Monitor Effectiveness	Consulted	Responsible	Accountable	Consulted	Informed
Independent Validation	Accountable	Informed	Consulted	Consulted	Responsible

Crucial Distinction: The SMT implements controls. The Board and ARC test and oversee them. Voluntary boards cannot rely on assumption.

2.2 Master RACI Governance Matrix

The matrix below defines the allocation of responsibilities across the five key governance tiers within a charity:

Governance / Control Lifecycle Stage	Trustees / Board	Audit & Risk Comm. (ARC)	CEO / SMT	Control Owners / Staff	Internal / Ext. Audit
Policy Drafting & Control Extraction	I	C	A	R	C
Policy Approval & Review Cycle	A	C / R	C	I	I
Internal Control Universe (ICU) Design	I	A	R	C	C
Daily / Monthly Control Execution	I	I	A	R	I
Digital Staff Attestation Compliance	I	I	A	R	I
Control Performance Testing & Logging	I	C	A	R	C
Risk Register Integration & Multipliers	A	R	C	I	C
Board Exception Dashboard Reporting	I	A / R	C	I	I
ISA 315 Walkthroughs & D&I Testing	I	C	A / R	R	R / A
Statutory Audit ISA 260 / 265 Review	A	R / C	C	I	R

GOVERNANCE PRINCIPLE: OVERLAY VS. EXECUTION

A critical principle of charity governance is the Segregation of Duties between Implementation and Oversight. Senior Management (SMT) is Accountable for implementing and testing controls, while the Board/ARC provides independent challenge. Trustees must never become 'Responsible' for executing daily operational controls, as this destroys their ability to provide objective oversight.

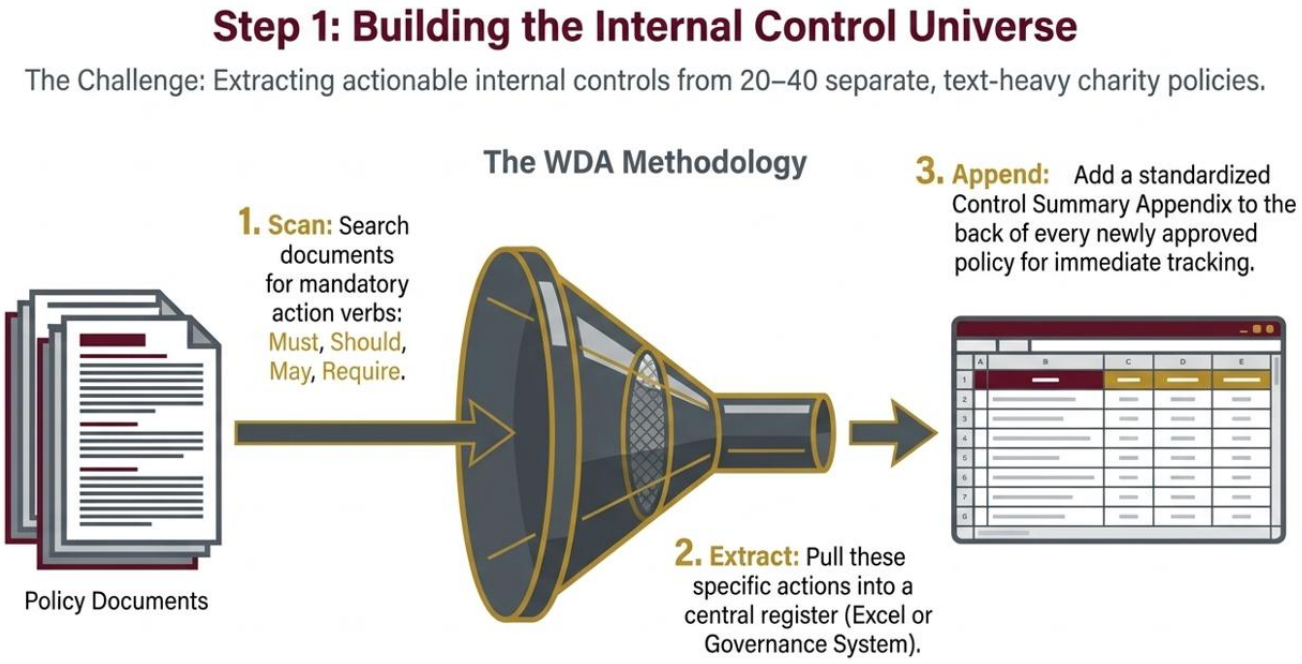
3. STEP-BY-STEP GUIDE TO BUILDING A CONTROL UNIVERSE

The Internal Control Universe (ICU) is a comprehensive master database that extracts every operational, financial, and regulatory mandate contained within a charity's approved policy suite and transforms them into tracked, verifiable control tasks.

3.1 Phase 1: Policy Audit & Keyword Extraction Methodology

Building the ICU begins with an exhaustive line-by-line audit of all 20 to 40 approved policy documents (e.g., Financial Management Policy, Procurement Policy, Safeguarding Policy, IT & Data Security Policy, HR Policy, Travel & Expenses Policy). Auditors scan text for key modal verbs:

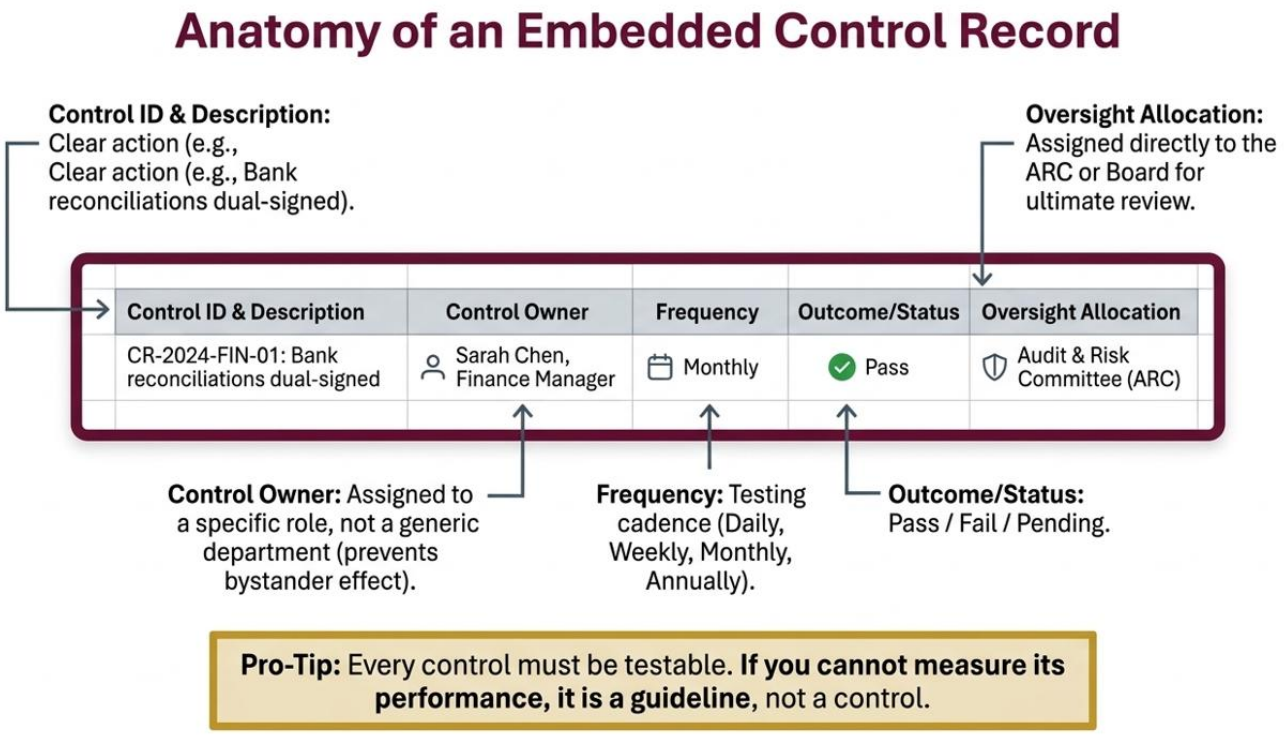
- **Keyword 'MUST':** Indicates a mandatory, non-negotiable operational control requirement (e.g., 'All purchase orders over €5,000 MUST be approved by two signatories'). Every 'MUST' statement creates an explicit control entry in the ICU.
- **Keyword 'SHOULD':** Indicates a strongly recommended best practice requirement (e.g., 'Bank reconciliations SHOULD be reviewed by the Finance Director within 5 working days of month-end'). Evaluated for operational feasibility and logged in the ICU.
- **Keyword 'MAY':** Indicates discretionary guidance. Evaluated to determine if formal control standardization is required.



3.2 Phase 2: Structuring the Master Control Register

Every extracted control item is populated into a standardized Master Control Register containing ten mandatory metadata fields:

- **1. Control ID:** Unique alphanumeric code (e.g., FIN-INC-001, HR-SAF-012).
- **2. Originating Policy:** Name and section of the originating board-approved policy.
- **3. Control Description:** Precise description of the required operational action.
- **4. Control Type:** Preventative (prevents errors/fraud before occurring), Detective (identifies errors/fraud after occurring), or Corrective.
- **5. Testing Frequency:** Daily, Weekly, Monthly, Quarterly, Bi-Annual, Annual, or Event-Driven.
- **6. Control Owner:** Named role responsible for performing and logging the control.
- **7. Evidential Proof:** Specific physical or digital documentation required to verify performance (e.g., signed reconciliation, system audit log, approved PO).
- **8. Oversight Body:** Designated committee or manager responsible for reviewing control effectiveness.
- **9. Linked Risk ID:** Specific organizational risk(s) mitigated by this control.
- **10. Effectiveness Status:** Effective (Green), Partially Effective (Amber), or Ineffective (Red).



Pro-Tip: Every control must be testable. **If you cannot measure its performance, it is a guideline,** not a control.

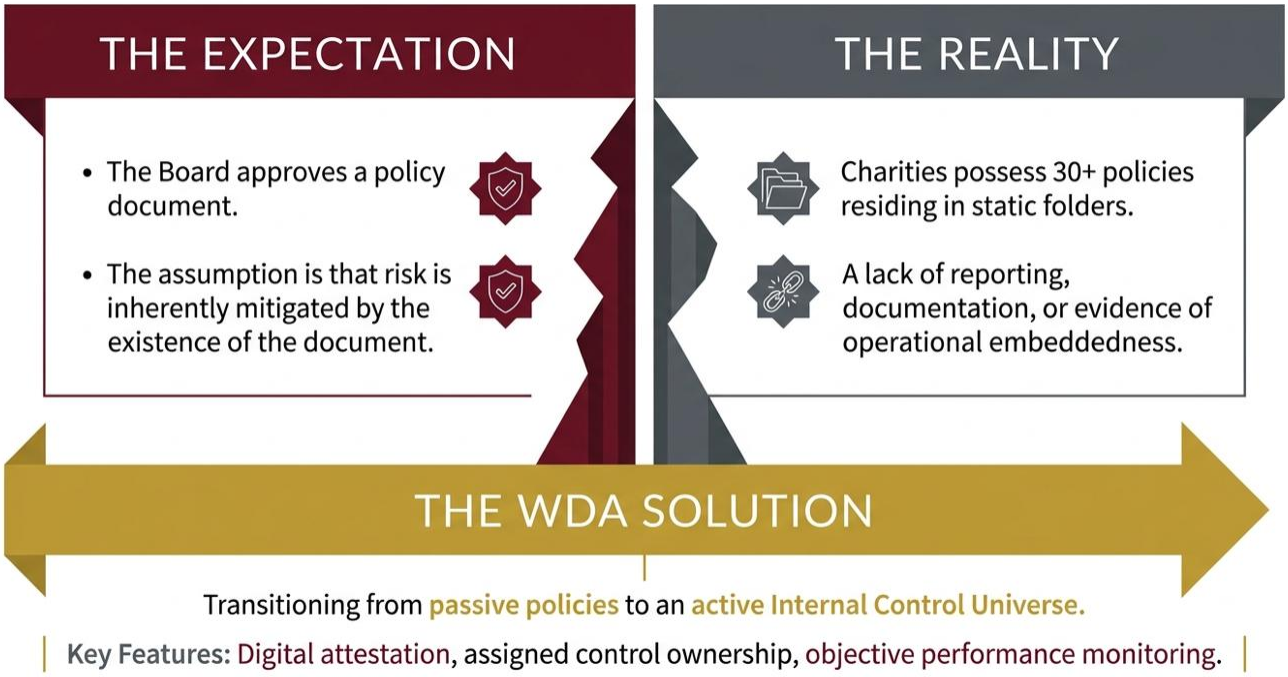
3.3 Sample Extract: Master Internal Control Universe

The table below illustrates a representative extract across five core charity operational domains:

Control ID	Domain & Policy	Control Action Description	Frequency	Control Owner	Evidential Proof Required
FIN-INC-001	Financial Mgmt (Income)	Dual counting and logging of all cash donations/events by two independent staff members.	Event-Driven	Fundraising Lead	Dual-signed cash tally sheets & bank deposit slip
FIN-BNK-004	Financial Mgmt (Banking)	Monthly bank reconciliations performed for all bank accounts and reviewed by CFO.	Monthly	Finance Officer / CFO	Signed bank statement & reconciliation report
FIN-EXP-008	Procurement Policy	Purchase orders >€5,000 require 3 competitive quotes and dual SMT approval.	Event-Driven	Procurement Manager	Quote summary sheet, 3 written quotes & dual PO
HR-SAF-002	Safeguarding Policy	Garda Vetting clearance secured before any employee or volunteer commences duties.	Pre-Hire	HR Officer	National Vetting Bureau clearance confirmation
IT-DAT-005	IT & Data Security	Quarterly review of user access permissions to financial software and payroll systems.	Quarterly	IT Administrator / CFO	System user access audit report & removal log

4. POLICY REGISTER GOVERNANCE & DIGITAL STAFF ATTESTATION

A major point of vulnerability in charity governance is staff unfamiliarity with approved policies. Maintaining a central Policy Register paired with a mandatory Digital Staff Attestation system ensures that policies remain active, updated, and enforceable across the entire organization.



4.1 Policy Register Architecture

Every charity must maintain a central, board-monitored Policy Register that tracks the lifecycle of every governance document. Policies must be assigned fixed review cycles (typically 12 months for high-risk financial/safeguarding policies; 24–36 months for general operational policies).

Policy Title	Policy Owner	Version	Approval Date	Next Review Date	Staff Attestation %
Financial Management Policy	CFO / Finance Comm.	v4.1	15-Jan-2026	15-Jan-2027	98.5%
Safeguarding & Child Protection	Head of Operations	v3.0	10-Jun-2025	10-Jun-2026	100.0%
Procurement & Tendering Policy	CFO	v2.2	18-Nov-2025	18-Nov-2026	94.2%
Data Protection & GDPR Policy	Data Protection Officer	v5.0	01-Mar-2026	01-Mar-2027	96.8%

4.2 Digital Staff Attestation System

To establish operational compliance, charities must implement automated digital sign-off workflows where staff, SMT, and volunteers formally log a digital 'Read and Understand' attestation. Attestations are triggered:

- **1. Onboarding:** Mandatory completion during new employee orientation prior to commencing operational duties.
- **2. Policy Revisions:** Automatic re-attestation requests dispatched to all relevant staff upon board approval of policy amendments.
- **3. Annual Cycle:** Annual digital refresher sign-offs across high-risk governance policies.

Digital Attestation



- Moving beyond emailed policies.
- Staff and SMT must digitally sign off that they have Read and Understood their assigned controls.
- Creates a psychological deterrent against fraud and a clear accountability paper trail.

The Policy Register

Essential metadata required for strict governance:

Policy Name	Document Owner	Version Control	Last Review Date	Next Scheduled Review Date

5. RISK REGISTER INTEGRATION & OBJECTIVE RESIDUAL SCORING

In traditional charity governance, assessing 'Residual Risk' on a Risk Register is highly subjective—often determined by verbal debate or instinct during board meetings. Integrating the Internal Control Universe with the Risk Register replaces guesswork with mathematically measured control performance.



5.1 Mathematical Risk Multiplier Framework

Every organizational risk is assigned an Inherent Risk Score (Impact x Likelihood = 1 to 25). The Residual Risk Score is calculated by applying an objective Control Multiplier based on the measured performance of linked internal controls:

Control Effectiveness Rating	Operational Performance Criteria	Control Multiplier	Risk Reduction %	Impact on Residual Risk Score
Robust / Effective (Green)	100% of controls tested performed on time with full evidential proof.	0.20	80% Reduction	Inherent Risk 20 → Residual Risk 4 (Low)
Strong (Green-Amber)	85%–99% of controls performed successfully; minor administrative delays.	0.40	60% Reduction	Inherent Risk 20 → Residual Risk 8 (Moderate)
Reasonable (Amber)	70%–84% of controls performed; non-critical control gaps identified.	0.60	40% Reduction	Inherent Risk 20 → Residual Risk 12 (Moderate)
Weak (Amber-Red)	50%–69% of controls performed; significant overdue controls or missing proof.	0.80	20% Reduction	Inherent Risk 20 → Residual Risk 16 (High)
Ineffective / Absent (Red)	<50% performed; critical control failures or unassessed controls.	1.00	0% Reduction	Inherent Risk 20 → Residual Risk 20 (Critical)

Objective Risk Scoring (The Assessment Engine)

Control Strength	Strength Factor	Inherent Risk Score	Residual Risk Score	Residual Risk Appetite
Robust	20%	25	5	Low
Strong	40%	25	10	Low
Reasonable	60%	25	15	Medium
Weak	80%	25	20	High
Ineffective	100%	25	25	High

Residual risk is no longer a guess—it is a mathematical output of your Control Universe's effectiveness.

OBJECTIVE RESIDUAL RISK DYNAMICS

WORKED EXAMPLE: A charity identifies 'Cyber Fraud & Phishing' with an Inherent Risk Score of 20 (Impact 5 x Likelihood 4). If quarterly access reviews and MFA controls are tested and rated 'Robust' (0.20 multiplier), Residual Risk drops to 4 (Green). However, if access reviews are overdue and rated 'Weak' (0.80 multiplier), Residual Risk automatically jumps to 16 (Red) on the Board Dashboard, immediately triggering mandatory corrective action.



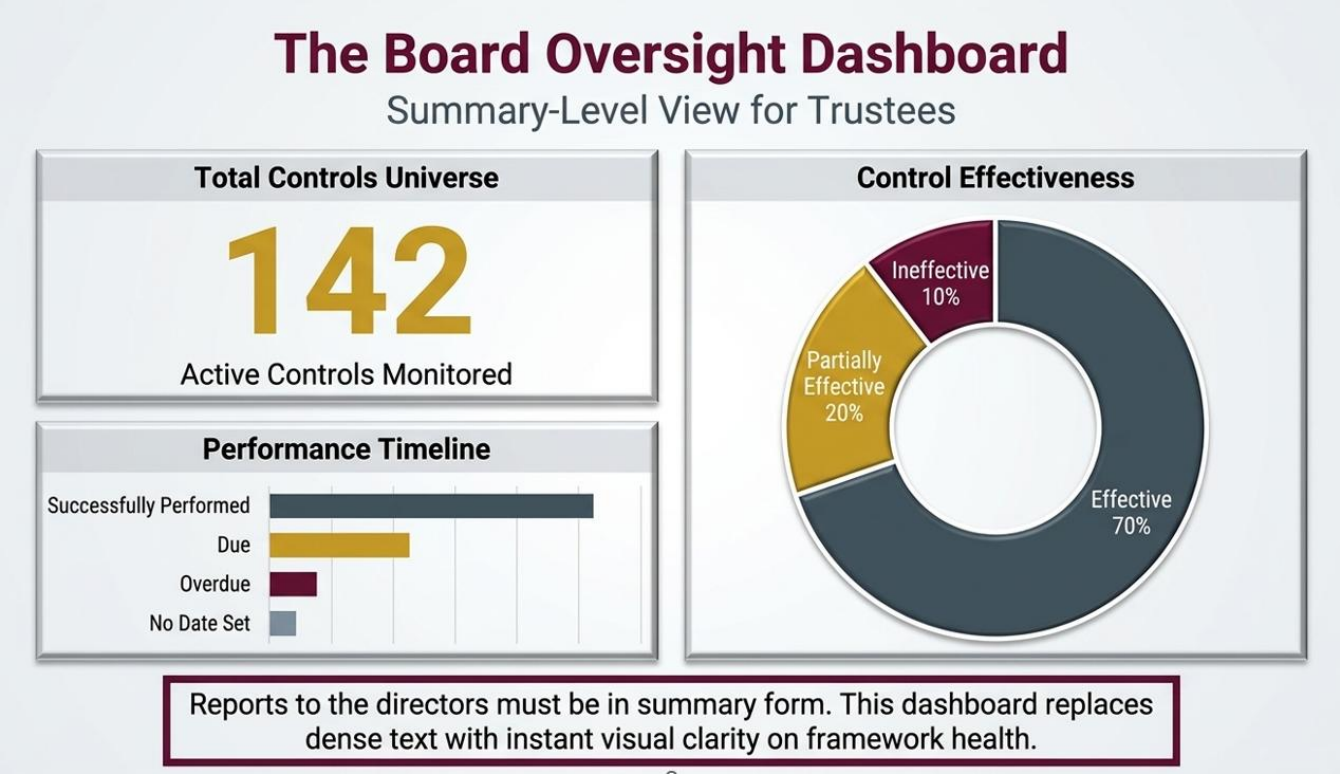
6. PERFORMANCE MONITORING & BOARD DASHBOARD

Board members do not have time to read hundreds of individual control logs. To enable efficient oversight, executive board packs must include a high-level Board Summary Dashboard, supported by a detailed Exception Report highlighting failing or overdue controls.

6.1 Executive Dashboard Specifications

The Board Dashboard synthesizes control performance into three core visual metrics:

Dashboard Metric Category	Key Performance Indicators (KPIs) Displayed	Strategic Governance Purpose
1. Execution Volume	• Total Adopted Controls (e.g., 142) • Controls Tested in Period (e.g., 128) • Testing Coverage % (e.g., 90.1%)	Verifies whether SMT is actively testing and documenting the control universe.
2. Schedule Compliance	• Performed On-Time (e.g., 115) • Due for Testing (e.g., 13) • Overdue Controls (e.g., 10, Red Flag) • No Date Set (e.g., 4)	Identifies operational bottlenecks and delays in management testing schedules.
3. Effectiveness Breakdown	• Green / Effective % (e.g., 82%) • Amber / Partially Effective % (e.g., 12%) • Red / Ineffective % (e.g., 6%)	Provides an instant snapshot of organizational control health for Board review.



6.2 Exception Reporting Protocol

Behind the summary dashboard, board packs must contain an Exception Report detailing every control rated Red (Ineffective) or Overdue. The Exception Report mandates four items: Root Cause Analysis, Corrective Action Plan, Assigned Owner, and Target Completion Date.

Behind the Dashboard: Managing Exceptions

Summary reporting is useless without actionable exception data. Accountability drives SMT to explain why approved policies are not being executed.

Control ID	Description	Why it Failed (Root Cause)	Control Owner	Suggested Mitigation	Next Retest Date	Linked Risks (Exposure point)
C-102	Segregation of Duties Violation: Payment Approvals	System configuration allowed single user dual approval for payments > $50k due to recent role update.	Finance Manager (J. Smith)	Immediate role access revocation; implement mandatory dual approval configuration; re-train finance team.	Oct 25, 2024	Financial Loss, Regulatory Non-Compliance
C-205	Unauthorized System Access Attempt	Legacy vendor account not disabled post-contract termination; detected by anomalous login location.	IT Security Lead (K. Sharma)	Disable all inactive vendor accounts; automate account offboarding process; review all active external access.	Oct 28, 2024	Data Breach, Operational Disruption
C-310	Incomplete Vendor Due Diligence	Procurement skipped mandatory background check for new software vendor due to project urgency.	Procurement Director (M. Davis)	Execute full due diligence immediately; establish hard stop in procurement workflow for incomplete checks.	Nov 01, 2024	Third-Party Risk, Reputational Damage
C-401	Failure to Encrypt Sensitive Data at Rest	New database instance deployed without default encryption enabled; overlooked during rapid deployment.	Cloud Infrastructure Lead (A. Chen)	Enable encryption on database; implement automated configuration audit for new instances.	Oct 31, 2024	Data Privacy Violation, Regulatory Fines
C-550	Missed Quarterly BCP Testing	Scheduled test for APAC region cancelled due to conflicting critical business operations; not rescheduled promptly.	Business Continuity Manager (R. Taylor)	Reschedule BCP test immediately; define clear criteria and authority for test cancellation and rescheduling.	Nov 15, 2024	Operational Resilience Failure, Business Interruption

This drill-down view highlights exact points of exposure, ensuring the Board does not get lost in the weeds while maintaining total operational oversight.

7. STATUTORY AUDIT ALIGNMENT

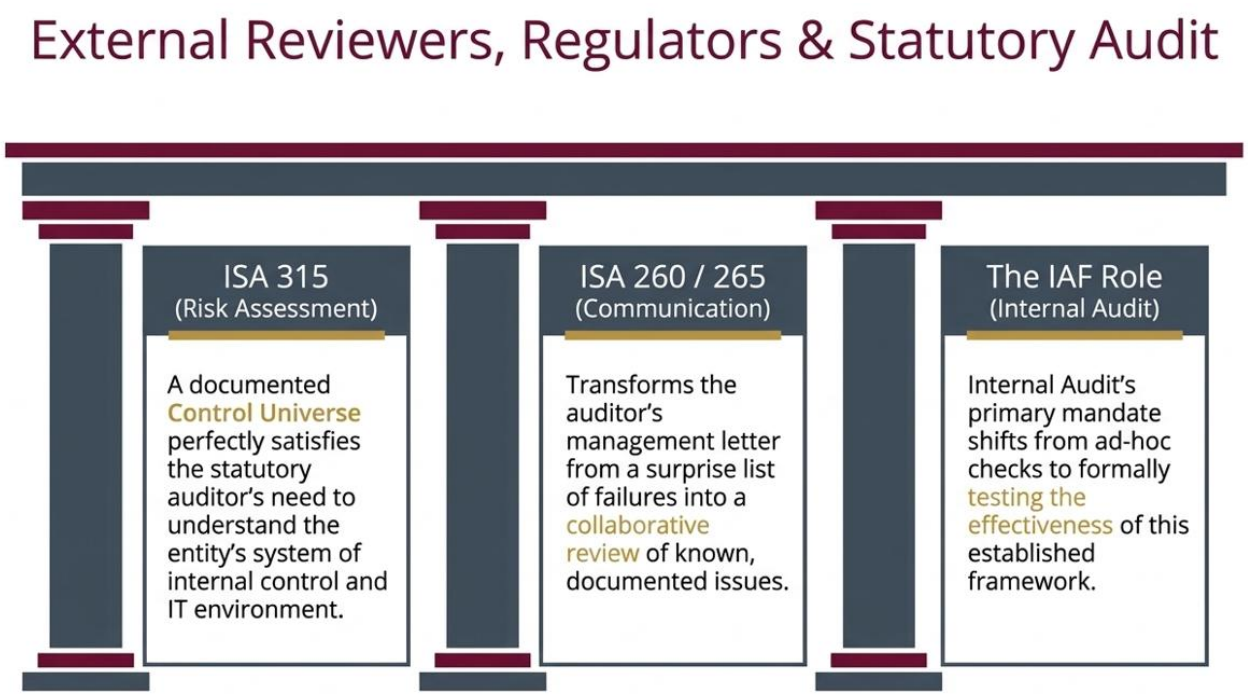
Establishing an Internal Control Universe provides profound benefits during the annual statutory audit. International Standards on Auditing (Ireland) require auditors to assess internal controls during financial statement audits. An active ICU provides verifiable audit evidence, reducing audit friction, management queries, and professional fees.

7.1 ISA 315: Design & Implementation (D&I) Walkthroughs

Under ISA (Ireland) 315 (Identifying and Assessing the Risks of Material Misstatement), the statutory auditor must evaluate the five components of the charity's internal control system:

- **1. Control Environment:** Board oversight, tone at the top, ethical values, and organizational structure.
- **2. Risk Assessment Process:** How management identifies operational and financial risks.
- **3. Information & Communication:** Financial reporting systems, accounting software, and communication channels.
- **4. Control Activities:** Authorization thresholds, segregation of duties, physical asset security, and IT controls.
- **5. Monitoring of Controls:** SMT and ARC review of ongoing control performance.

Auditors perform 'Walkthrough Tests' at the planning stage to verify Design & Implementation (D&I). When a charity presents an active ICU with documented proof for each control, the auditor can evaluate D&I rapidly and determine whether to adopt a 'Controls Reliance Strategy' (reducing substantive detail testing).



7.2 Mapping Internal Controls to Financial Statement Assertions

Statutory auditors test financial statement line items against specific directors assertions. The table below illustrates how specific internal controls directly satisfy ISA audit assertions:

Financial Statement Area	ISA Audit Assertion	Corresponding Internal Control Mechanism
Income / P&L	Occurrence	Dual-signed cash donation sheets and official receipt logs verify events occurred.
Income / P&L	Completeness	Pre-numbered grant agreements cross-referenced to bank lodgements ensure no income omitted.
Expenditure / P&L	Accuracy	3-way matching of Purchase Order, Goods Received Note, and Supplier Invoice before payment.
Expenditure / P&L	Classification	Standardized Chart of Accounts mapping reviewed monthly by Finance Committee.
Expenditure / P&L	Cut-Off	Year-end invoice cut-off testing and accrual log review by CFO.
Balance Sheet	Existence	Annual physical verification and tagging of fixed assets against Fixed Asset Register.
Balance Sheet	Rights & Obligations	Grant agreement repository confirming restricted fund ownership and obligations.
Balance Sheet	Valuation & Allocation	Quarterly bad debt provision review and asset impairment assessments.
Balance Sheet	Completeness	Monthly bank reconciliations covering all bank, credit card, and petty cash accounts.

7.3 ISA 265 & ISA 260 Auditor Communication Protocols

- **ISA 265 (Communicating Deficiencies):** Mandates that statutory auditors communicate significant deficiencies in internal control in writing to Those Charged with Governance (Trustees/ARC). An active ICU prevents control breakdowns, eliminating formal written deficiency letters.
- **ISA 260 (Governance Communication):** Requires two-way dialogue between auditor and trustees regarding audit scope, significant risks, accounting policies, and uncorrected misstatements.
- **ISA 450 & Materiality:** Governs evaluation of misstatements. Overall Materiality is typically set at 1.0% of Total Revenue/Expenses (e.g., €50k on €5M income), Performance Materiality at 75% (€37.5k), and Clearly Trivial at 5% (€2.5k). Strong controls ensure uncorrected misstatements stay well below trivial limits.

8. FRAUD PREVENTION, CYBERCRIME & MANAGEMENT OVERRIDE SAFEGUARDS

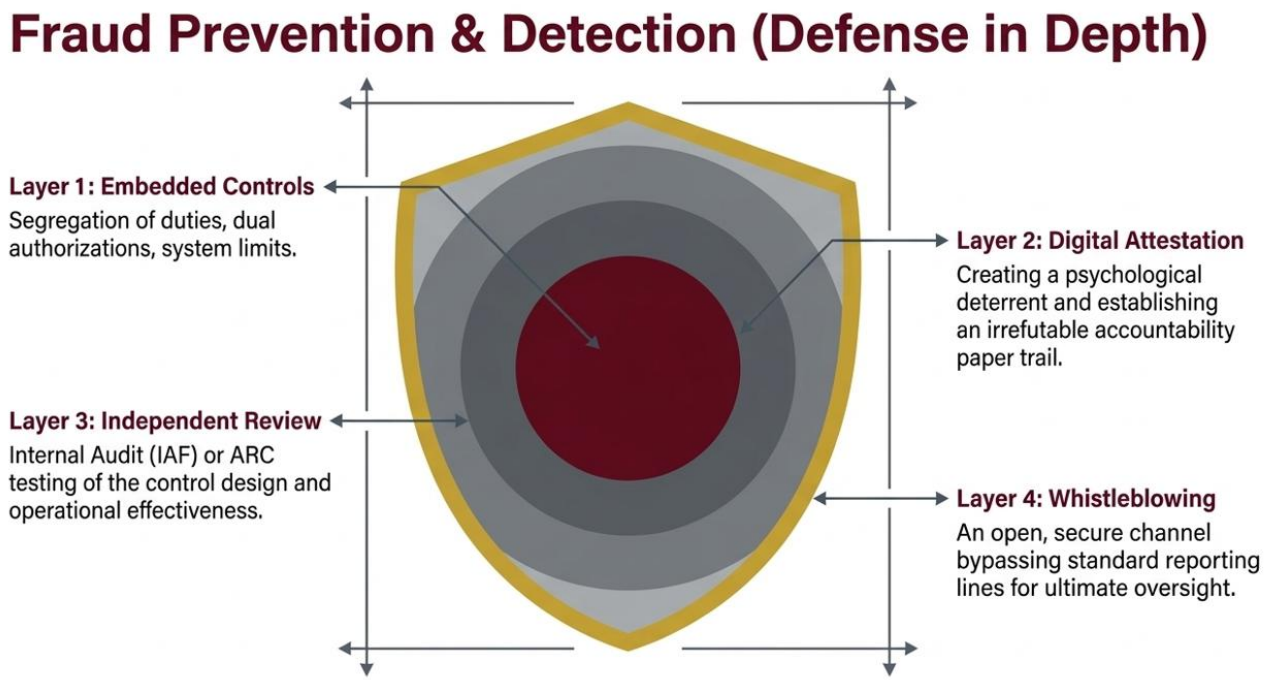
Charities are prime targets for financial fraud, cybercrime, and mandate manipulation due to public trust and high transaction volumes. A robust Internal Control Universe embeds specific preventative safeguards to combat key sector fraud vectors.

8.1 High-Risk Charity Fraud Vectors & Embedded Safeguards

- **1. Supplier Mandate Fraud:** Fraudsters impersonate legitimate suppliers requesting changed bank details. Safeguard: Mandatory independent telephone verification using existing registered numbers before updating supplier bank records.
- **2. Online Banking & Cyber Fraud:** Unauthorized transfer of charity funds. Safeguard: Dual-signatory online banking setup requiring independent approval on separate devices for all transfers >€1,000.
- **3. Fundraising & Cash Leakage:** Diversion of unrecorded cash donations. Safeguard: Dual-sealed collection boxes, immediate two-person counting, pre-numbered receipts, and same-day bank lodgments.
- **4. Management Override of Controls:** Senior executives bypassing established controls. Safeguard: Independent ARC review of all post-close journal entries, CEO expense claims approved by Board Chair, and strict approval limits.

8.2 Whistleblowing Protections & Protected Disclosures

Under the Charities Act 2009 and Protected Disclosures legislation, charities must maintain a formal Whistleblowing Policy. Staff must be provided with secure, confidential channels (including direct access to the ARC Chair) to report financial irregularities without fear of penalization.



9. INTERNAL AUDIT FUNCTION

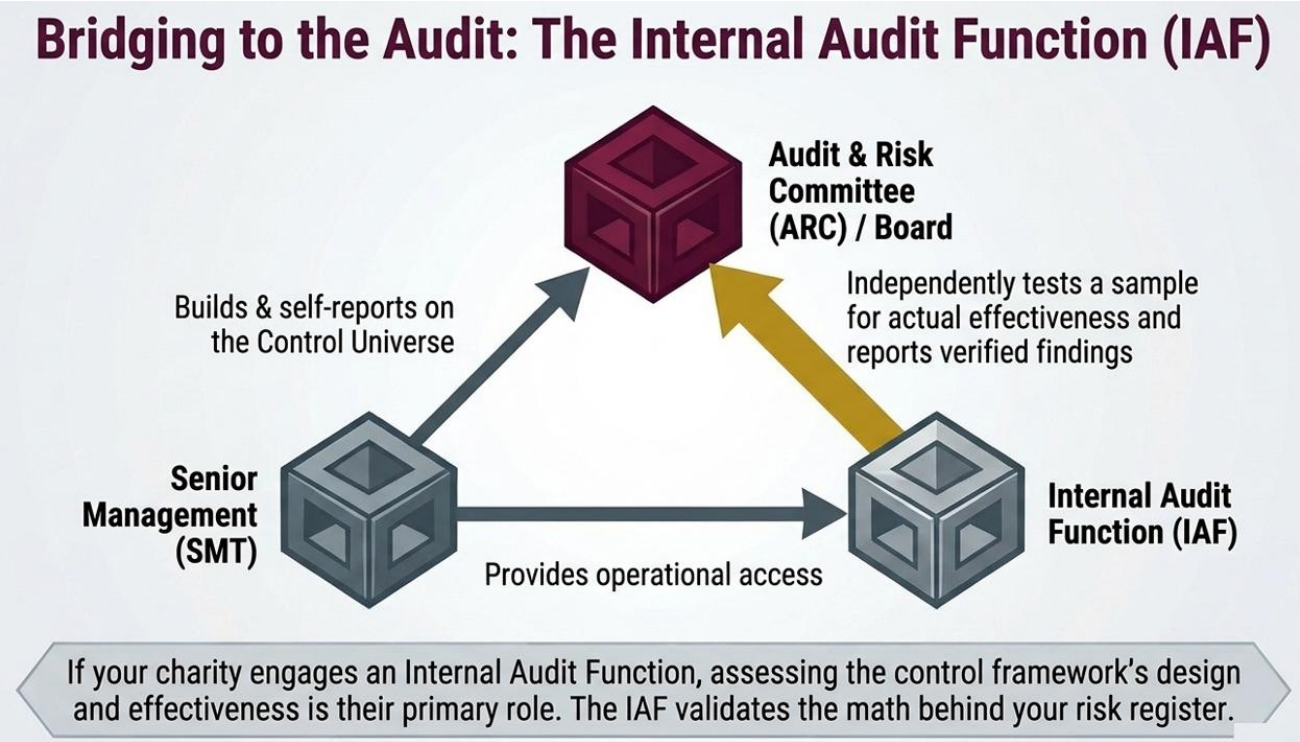
For larger or more complex charities, establishing an Internal Audit Function (IAF)—either in-house or outsourced—provides essential 'Third Line of Defense' assurance to the Board of Trustees.

9.1 The Three Lines of Defense Model

- **First Line:** Operational Management and Staff executing daily internal controls (Control Owners).
- **Second Line:** Risk Management, Compliance Officers, and SMT oversight functions monitoring control universe performance.
- **Third Line:** Internal Audit Function providing independent, objective evaluation of control design and operating effectiveness.

9.2 Developing a Risk-Based Internal Audit Plan (RBIA)

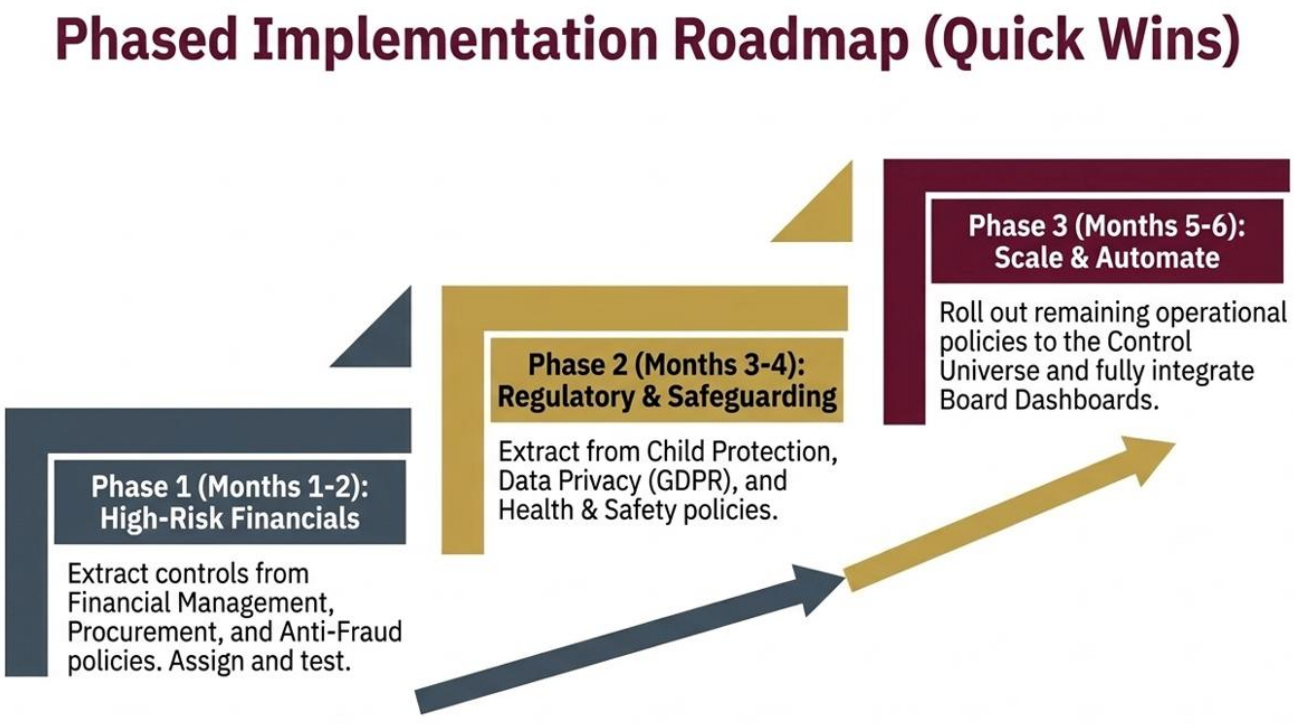
The IAF uses the Internal Control Universe and Risk Register to formulate an annual Risk-Based Internal Audit Plan. The IAF conducts deep-dive thematic audits across high-risk areas (e.g., Procurement Audit, Grant Compliance Review, IT Security Audit), reporting findings directly to the Audit & Risk Committee.



10. PHASED 12-MONTH IMPLEMENTATION ROADMAP

Attempting to build an Internal Control Universe across all 40 policies simultaneously can overwhelm staff. WDA recommends a structured, 4-Phase implementation roadmap over 12 months:

Implementation Phase	Timeframe	Core Operational Focus & Deliverables	Target Governance Milestones
Phase 1: Quick Wins & High-Risk Core	Months 1–3	Audit Top 5 High-Risk Policies (Banking, Expenditure, Income, Safeguarding, IT). Extract controls into Master Register.	Board approval of ICU Framework & Phase 1 Control Register.
Phase 2: Full Policy Suite Rollout	Months 4–6	Audit remaining 20–35 policies (HR, Travel, GDPR, Governance). Launch Policy Register & Digital Staff Attestation.	100% staff digital attestation completion across core policies.
Phase 3: Risk & Dashboard Integration	Months 7–9	Link Control Universe to Risk Register. Implement Control Multipliers. Build Board Dashboard & Exception Reports.	First Executive Dashboard presented to ARC and Board.
Phase 4: Embedding & IAF Oversight	Months 10–12	Conduct full annual control performance review. Prepare ISA 315 audit packs. Launch thematic IAF reviews.	Statutory auditor reliance on ICU; full annual review completed.



11. COMMON SECTOR PITFALLS

WDA's advisory work across the charity sector highlights ten recurring pitfalls that undermine internal control effectiveness:

- **1. The Policy-in-a-Drawer Fallacy:** Believing that passing a policy at a board meeting equals operational compliance without subsequent testing.
- **2. Information Overload / Low-Signal Board Packs:** Presenting 50-page financial reports to trustees without high-level summary KPIs or exception highlighting.
- **3. Trustee Operational Creep:** Trustees becoming involved in approving daily payments, destroying their independent oversight role.
- **4. Single-Point-of-Failure Dependencies:** Failing to enforce dual sign-offs or independent reconciliations in small or volunteer-led teams.
- **5. Missing Staff Attestation Loops:** Allowing staff to work for months or years without formally confirming policy understanding.
- **6. Subjective Risk Scoring:** Treating risk register scoring as a subjective debate rather than linking scores to measured control logs.
- **7. Cash & Event Income Vulnerabilities:** Failing to maintain pre-numbered receipt logs or dual-counting protocols for fundraising events.
- **8. Informal Supplier Mandate Changes:** Updating bank details on email request without independent call-back verification.
- **9. Unchecked Management Override:** Allowing executive directors to approve their own expense claims or post unreviewed journal entries.
- **10. Statutory Audit Misalignment:** Viewing statutory audit as an adversarial hurdle rather than leveraging ISA 315 to strengthen governance.

12. STRATEGIC RECOMMENDATIONS

To achieve exemplary governance and ensure complete operational assurance, WDA provides the following actionable recommendations:

- **Recommendation 1: Formally Commit to ICU Paradigm —** Formally adopt the Internal Control Universe (ICU) methodology as the charity's core operational control framework.
- **Recommendation 2: Empower ARC Oversight —** Establish a dedicated Audit & Risk Committee (ARC) chaired by a qualified financial expert to oversee control universe monitoring.
- **Recommendation 3: Embed Board Dashboard Reporting —** Mandate that every board pack includes the 3-Metric Executive Dashboard and Exception Report.
- **Recommendation 4: Automate Digital Attestations —** Deploy a digital staff portal for automated 'Read and Understand' sign-offs upon hiring and post-policy revisions.
- **Recommendation 5: Objective Risk Register Scoring —** Implement the Control Multiplier matrix to ensure residual risk scores reflect true control performance.
- **Recommendation 6: Fortify Fraud & Mandate Controls —** Institute mandatory phone verification for supplier bank changes and dual-authorization banking controls.
- **Recommendation 7: Proactive Statutory Audit Alignment —** Engage early with statutory auditors, sharing the ICU pack to streamline ISA 315 D&I testing and ISA 265 review.
- **Recommendation 8: Annual Control Universe Refresh —** Conduct a full annual review of the Master Control Register, updating policies to reflect operational changes.

13.0 ABOUT WDA

- We are a mid-tier firm with two offices servicing our client bases in Dublin and Meath.
- WDA specialise in the provision of professional audit and consultancy services including to the Charity & Not for Profit Sector, with over 150 Charity clients across all sectors of the industry.
- Our professional staff comprises of 30 staff: - 4 Partners, 20 professional staff including 2 Audit Managers and 4 support/admin staff.
- Whelan Dowling & Associates has been providing audit and accounting services to the charity sector for over 40 years and are affiliated with the Chartered Accountants Ireland.
- Whelan Dowling & Associates (WDA) are an award-winning firm having achieved the "Best Medium Sized Accountancy Practice in Ireland in **May 2023** and ***again*** in **May 2026,** whilst also being named runner-up as best overall firm in Ireland for both years. We have also won best use of technology and have been shortlisted as a finalist many times over the past 10 years.
- WDA have acted as a Technical Assessor for the Good Governance Awards for several years,
- WDA is listed as a supplier of Audit and Professional services with the Charities Institute of Ireland.

Disclaimer This document, *Building Effective Charity Internal Controls: A Practical Guide*, is prepared by Whelan Dowling & Associates (WDA) for general guidance purposes only and does not constitute professional accounting, legal, or audit advice. While every effort has been made to ensure the accuracy of the information regarding the FRS102, Companies Act 2014 and the Charities SORP, this guide is not a substitute for independent professional advice tailored to your charity's specific circumstances. As outlined in this guide, the responsibility for implementing a control framework is a non-delegable duty of the trustees. Consequently, WDA accepts no liability for any loss or damage occasioned to any person acting or refraining from action as a result of any material in this publication. Trustees should consult with their auditors or professional advisors to ensure compliance with their specific statutory and fiduciary obligations.



