IT Governance 'In English': A Practical Guide for Charity Trustees & Management



www.wda.ie

CONTENTS

Executive Summary & Roadmap 3

1.0 Introduction: The Digital Imperative for Charities 4

2.0 The Governance Mandate: Defining Leadership Roles in IT Oversight 6

3.0 Common Weaknesses in Charity IT Governance 8

4.0 The Core Pillars of Effective IT Governance 9

- 4.1 Strategic Alignment 9
- 4.2 Comprehensive Risk Management 10
- 4.3 Information Security & Cybersecurity 11
- 4.4 Business Continuity & Resilience 12
- 4.5 Oversight of Outsourced IT Functions 13
- 4.6 Compliance & Legal Obligations 14

5.0 A Practical 12-Month Roadmap to Better Governance 15

- Quarter 1: Foundation & Assessment 15
- Quarter 2: Control Implementation 15
- Quarter 3: Detection & Response 16
- Quarter 4: Testing & Improvement 16

6.0 Summary and Key Recommendations 17

Appendix 1: Sample IT Risk Appetite Statement 18

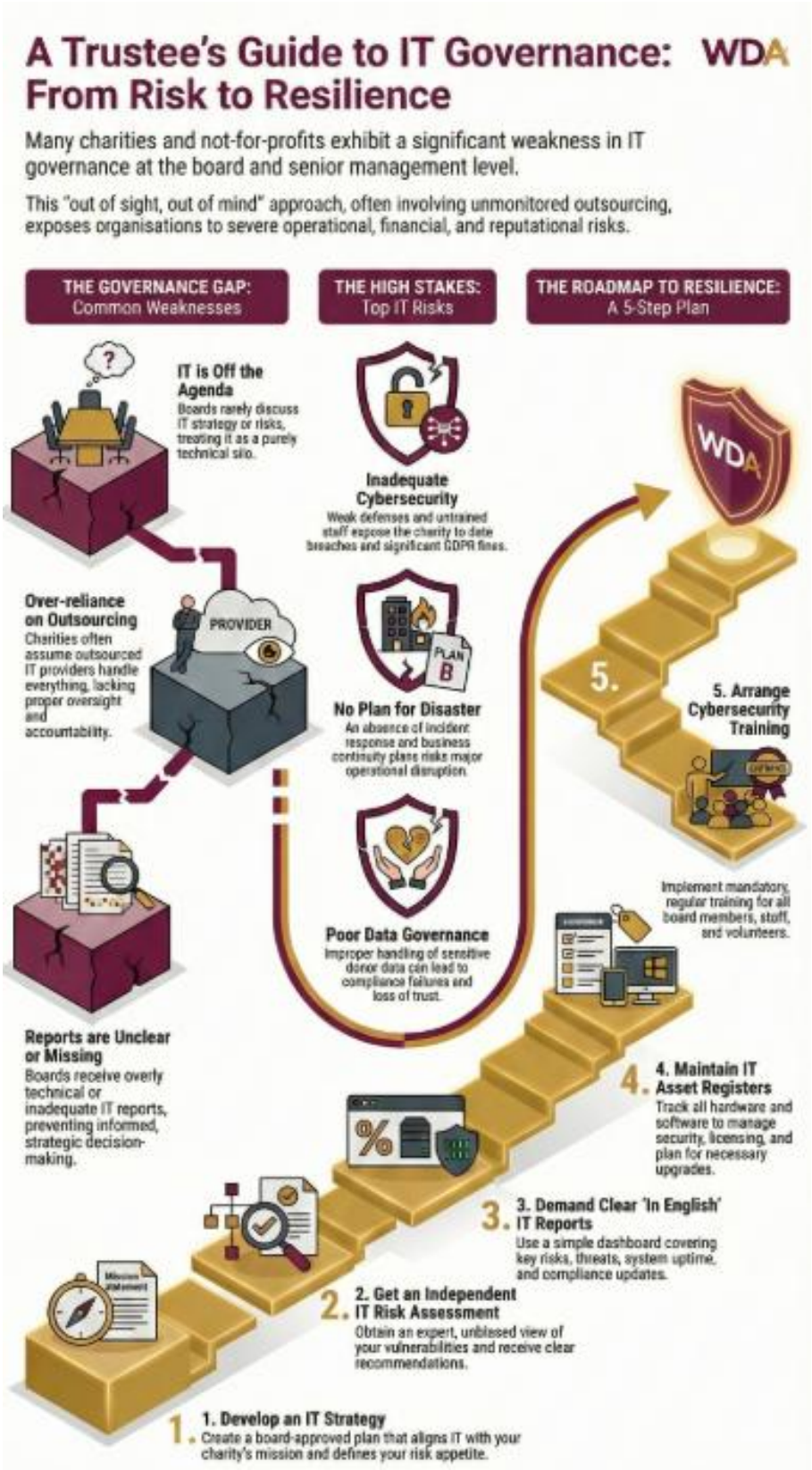
- Statement of Philosophy 18
- Specific Risk Areas & Appetite 18
- Key Risk Indicators (KRIs) & Tolerances 18

Appendix 2: Sample Questions For Trustees to Demonstrate IT Oversight 19

- 1. Strategy and Alignment 19
- 2. Risk Management & Appetite 19
- 3. Cybersecurity & Incident Response 19
- 4. Outsourcing & MSP Oversight 20
- 5. Business Continuity & Resilience 20
- 6. Asset & Data Management 20

Appendix 3: Sample IT Risk Register Assessment Template 21

EXECUTIVE SUMMARY & ROADMAP



1.0 INTRODUCTION: THE DIGITAL IMPERATIVE FOR CHARITIES

Executive Summary: The Strategic Imperative

The Problem:
Many Boards treat IT as a utility rather than a strategic enabler. Reliance on Managed Service Providers (MSPs) often creates a false sense of security—"Out of sight, out of mind."

The Risks:
Passive governance leads to a hidden accumulation of risks, including cybercrime, data breaches (GDPR), and regulatory non-compliance.

The Solution:
Governance is not management. The Board must move from passive acceptance to active challenge, focusing on alignment, risk appetite, and value delivery.

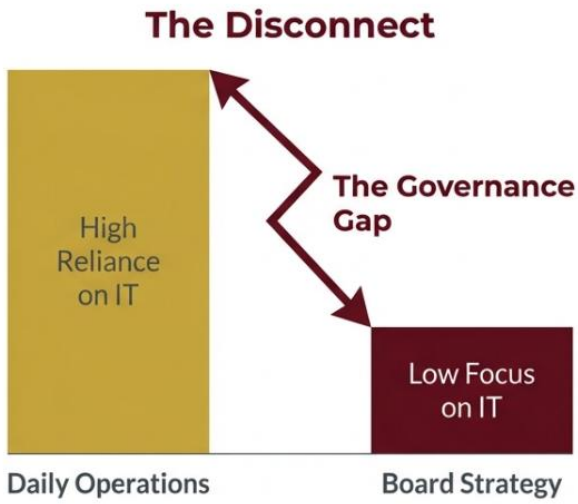
Key Takeaway:
IT Governance is not about fixing computers. It is about ensuring IT delivers value to the enterprise and supports sustainable growth.

In the modern not-for-profit sector, information technology (IT) has evolved from a back-office utility into a core enabler of charitable purpose. From managing donor data and delivering services to coordinating volunteers and ensuring regulatory compliance, charities are now significantly more reliant on IT systems to function effectively. Despite this deep operational dependence, a critical gap often exists between the use of technology and the strategic oversight provided by Boards of Trustees and Senior Management Teams (SMT). This gap can expose an organisation to significant financial, operational, and reputational risks.

The Current Landscape: The 'Governance Gap'

Key Insight: A critical weakness exists in the Not-For-Profit sector regarding IT Governance at Board and SMT levels.

- **Out of Sight, Out of Mind:** Blind reliance on Managed Service Providers (MSPs) without oversight.
- **Static Agendas:** IT is rarely discussed unless something breaks.
- **The Exposure:** Operational paralysis, reputational damage, and financial loss.



This guide addresses a common but dangerous organisational challenge: an "out of sight, out of mind" approach where IT is viewed as a technical expense rather than a strategic asset. Drawing on cross-industry best practices and regulatory guidance, it provides a practical framework for charity trustees and senior leaders to establish robust IT governance.

The objective is to move beyond passive reliance on technology and outsourced providers toward a model of active, strategic control, ensuring that IT capabilities are fully aligned with the charity's mission and risk appetite.

To achieve this, this report defines the distinct governance roles of the Board, SMT, and external providers. It then identifies the common weaknesses that undermine effective oversight in the sector, details the core pillars of a strong governance framework, and concludes with a practical, step-by-step roadmap for measurable improvement.

The Current Landscape: “Out of Sight, Out of Mind”

The Reality:
Boards rarely discuss IT risks. Agendas are static, and board packs contain limited or unintelligible information.

The Fallacy:
“We have an IT guy/MSP, so we are safe.” This assumption ignores that MSPs focus on execution, not strategy.

The Consequence:
Hidden risks accumulate, including technical debt, security vulnerabilities, and compliance gaps.

“Weakness Identified: Board minutes often reflect little discussion on IT-related matters despite heavy reliance on technology.”



2.0 THE GOVERNANCE MANDATE: DEFINING LEADERSHIP ROLES IN IT OVERSIGHT

Clearly defined roles and responsibilities are the bedrock of effective IT governance. This is not about trustees becoming technical experts; it is about establishing a framework for strategic direction, risk management, and accountability. These are fundamental duties of any charity trustee.

As outlined in the Charities Governance Code, trustees have a legal responsibility to manage their charity's resources responsibly and act with reasonable skill and care. In an era where data and systems are among a charity's most critical assets, this mandate unequivocally extends to the governance of information technology.

The Board of Trustees/Directors	The Senior Management Team (SMT)	The Managed Service Provider (MSP)
Strategic Oversight: Sets the organisation's overall business strategy and risk appetite, ensuring the IT strategy is fully aligned with and capable of supporting charitable objectives.	**Operational Management:** Implements the board-approved business and IT strategies on a day-to-day basis, managing resources and personnel effectively.	**Technical Delivery:** Provides and manages the IT infrastructure and services as defined in the Service Level Agreement (SLA).
Risk Appetite: Formally defines and approves the level and types of IT risk the organisation is willing to accept to achieve its goals.	**Risk Implementation:** Manages IT risks within the board-approved appetite, ensuring that controls are implemented, monitored, and effective.	**Technical Risk Mitigation:** Implements specific technical controls (e.g., firewalls, patching, backups) to meet security and operational requirements.
Accountability: Holds the SMT accountable for the performance of the IT function and the management of associated risks. Reviews and challenges reports on IT performance, projects, and incidents.	**Reporting & Escalation:** Provides the Board with clear, comprehensible, and regular reports on key IT risks, major projects, and significant incidents. Escalates issues that fall outside the agreed risk appetite.	**Performance Reporting:** Delivers performance reports to the SMT as specified in the SLA, detailing service uptime, incident response times, and other key metrics.
Resource Allocation: Ensures sufficient resources (budget, staff, expertise) are allocated to execute the IT strategy and manage risks effectively.	**Vendor Management:** Manages the relationship with the MSP, monitoring performance against the SLA and conducting regular due diligence.	**Service Provision:** Delivers IT services according to the agreed-upon standards, scope, and quality defined in the contract.

Defining IT Governance
It’s Not Just Tech Support

IT Governance is the framework ensuring that IT supports the organization’s goals, manages risks effectively, and delivers value to donors and beneficiaries.

IT Management (Operational)

Is the server working?
Are patches applied?
Is the helpdesk responsive?

Fixing

IT Governance (Strategic)

Does technology support our mission?
What is our risk appetite?
Are we compliant with GDPR?

Leading

The Charities Governance Code places a clear duty on trustees to "**Manage your charity’s resources responsibly**" and "**Act with reasonable skill and care**." IT infrastructure, software, and the data they contain are critical organisational resources. Failing to provide strategic oversight of these assets is a failure to meet these core duties. Trustees must ensure they have sufficient knowledge to understand the IT-related risks facing the charity and can demonstrate that these risks are being properly managed.

This clear delineation of roles provides a powerful framework for governance. However, the reality in many charities often falls short, leading to common and predictable weaknesses.

Who Does What? The Accountability Matrix

You can outsource the work, but you cannot outsource the accountability.

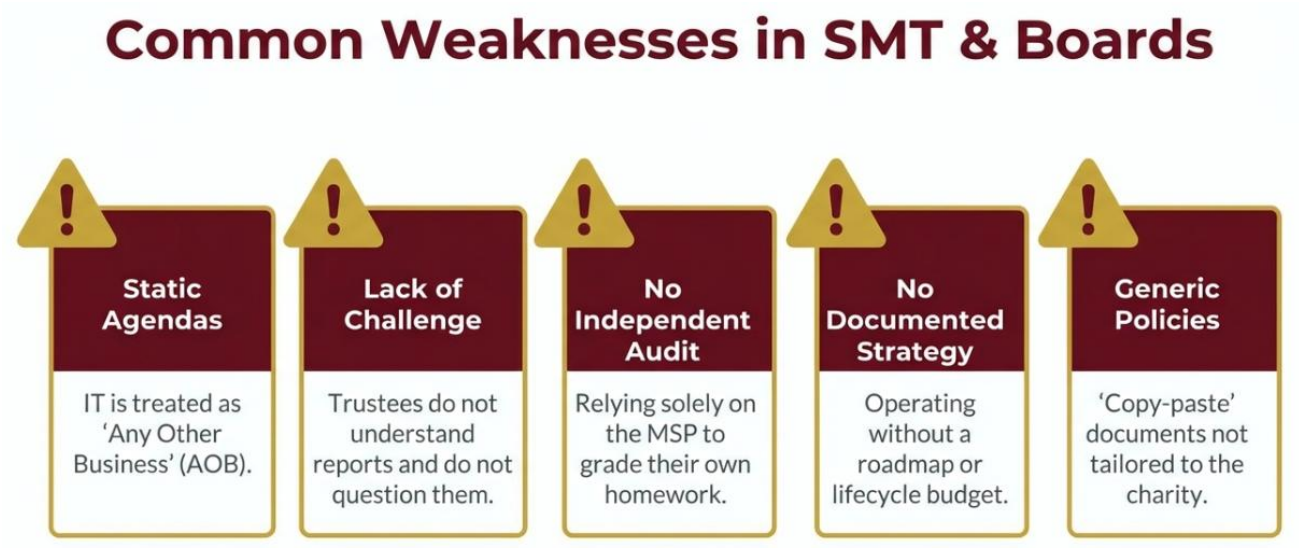
Managed Service Provider (MSP) Technical Execution	Senior Management Team (SMT) Operational Bridge	Board of Trustees Strategic Oversight
○ System availability	○ Translating strategy to IT initiatives	○ Setting risk tolerance
○ Patching & Security updates	○ Vendor performance management	○ Approving major investments
○ Incident response	○ Budget oversight	○ Ensuring regulatory compliance
○ Adhering to SLAs	○ Internal policy implementation	○ Holding SMT accountable

3.0 COMMON WEAKNESSES IN CHARITY IT GOVERNANCE

Recognising common governance challenges is the first step toward remediation and strengthening organisational resilience. The following weaknesses, identified through supervisory reviews across multiple sectors, serve as a diagnostic tool for Boards and SMTs to assess their own practices.

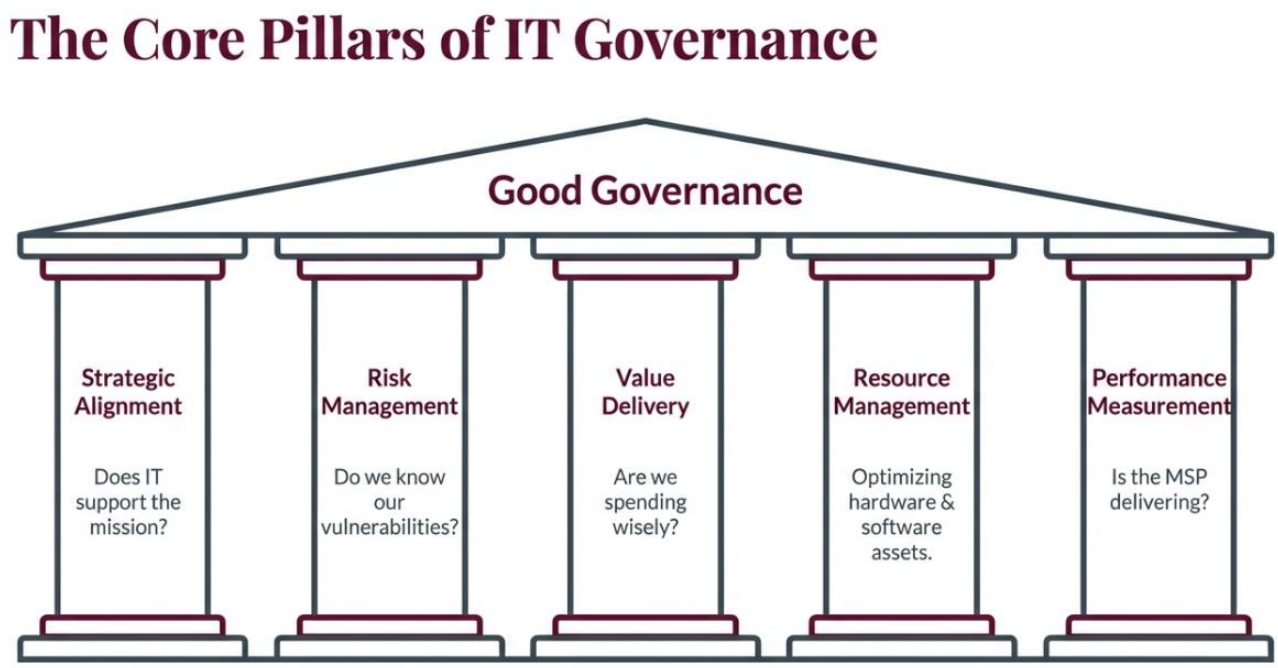
- **Lack of Strategic Alignment:** The IT strategy is disconnected from the charity's overall mission and business plan, resulting in technology that is unable to support strategic ambitions.
- **Absence from the Board Agenda:** Board minutes and agendas reflect little to no substantive discussion on critical IT matters, including strategy, major projects, or significant risks.
- **Insufficient Reporting:** The Board and SMT receive IT reports that are overly technical, infrequent, or lacking in the necessary detail to facilitate informed decision-making and effective challenge.
- **Passive Oversight of Outsourcing:** An over-reliance on third-party Managed Service Providers (MSPs) exists without adequate due diligence, ongoing performance monitoring, or robust Service Level Agreements (SLAs).
- **Fragmented Risk Perspective:** The organisation fails to take a holistic view of IT risks, leading to poor identification of threats, inadequate monitoring, and ineffective mitigation strategies.
- **Underinvestment and Legacy Systems:** IT is viewed as a cost centre rather than a strategic enabler, leading to chronic underinvestment and a dangerous reliance on outdated technology with known security vulnerabilities.

These issues create significant vulnerabilities. The following section provides a structured framework built on proven best practices to address these weaknesses systematically.



4.0 THE CORE PILLARS OF EFFECTIVE IT GOVERNANCE

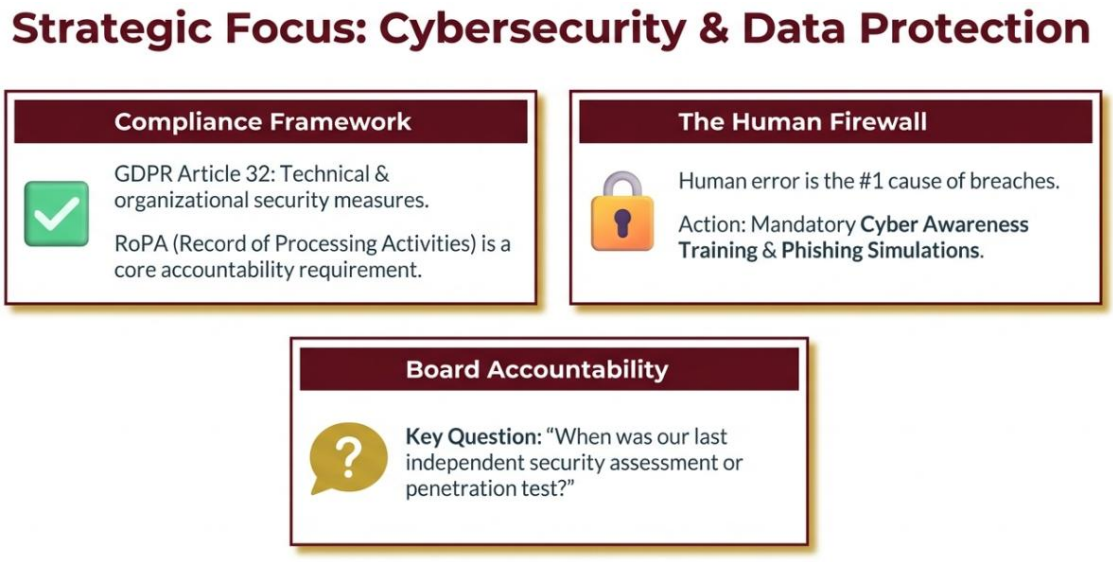
A robust IT governance framework is not a single policy but a system of interconnected pillars. These pillars, drawn from regulatory best practices, provide a comprehensive structure that enables a Board to exercise effective control, manage risk, and ensure that technology truly serves the organisation's charitable purpose.



4.1 Strategic Alignment

The most fundamental pillar of good governance is ensuring the IT strategy is explicitly aligned with the charity's overall business strategy. Technology must be positioned to support both current operations and the future direction of the organisation. An IT strategy developed in isolation is destined to fail.

The Board and SMT must ensure the IT strategy is a documented, board-approved plan. This plan must explicitly address the resources required for its execution, including an adequate IT budget, appropriate staffing levels and expertise, and a clear plan to identify and address any capability gaps that could obstruct strategic objectives.



4.2 Comprehensive Risk Management

Effective IT Risk Management is not a one-time assessment but a continuous and proactive process. It must be an integral component of the charity's overall operational risk management framework, providing a clear line of sight between people, processes, and the IT systems that support them.

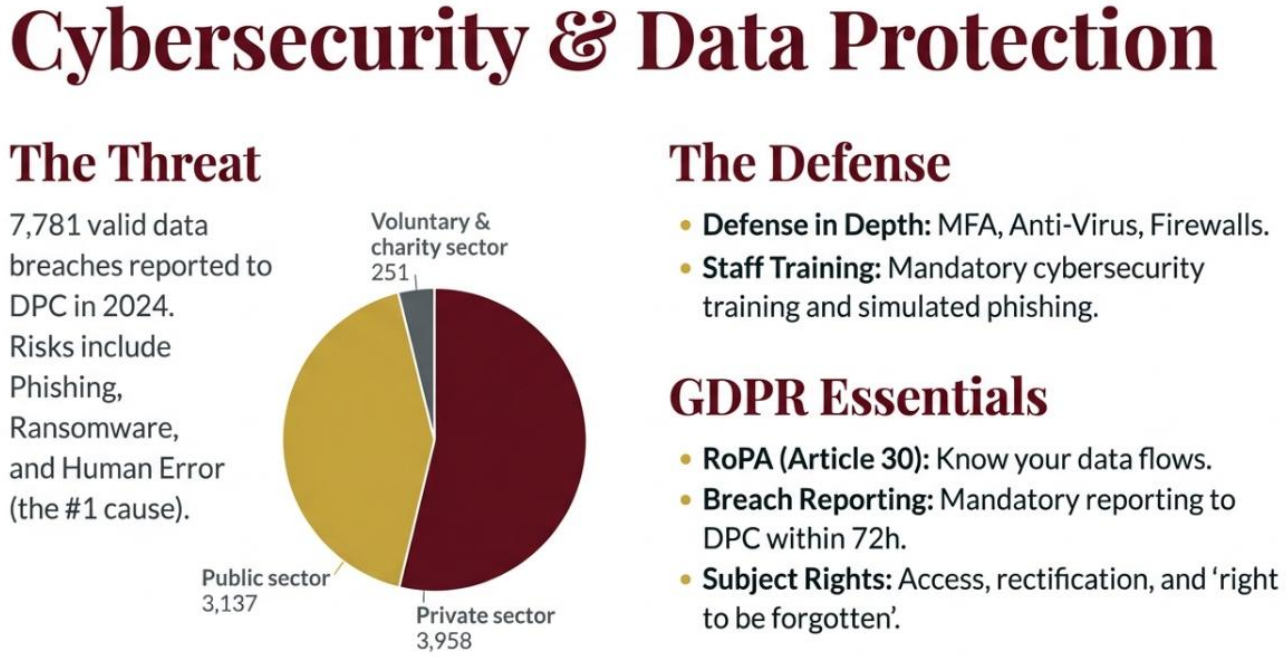


To achieve this, the organisation must implement a formal IT Risk Management (ITRM) framework. Its essential components include:

- A comprehensive **IT Risk Register** to formally identify, prioritise, assess, and manage risks in a structured manner.
- A complete **Inventory of IT Assets** (including hardware, software, and data), classified by their criticality to the business.
- A formal **Data Classification Framework** to ensure that critical or sensitive data is correctly identified and adequately safeguarded.
- An **Incident Management Plan** that establishes clear processes for the detection, notification, and escalation of IT incidents.

4.3 Information Security & Cybersecurity

Cybersecurity is a critical and non-negotiable component of IT risk management. Charities are prime targets for cyber criminals, who may seek to steal and sell sensitive personal data or to hold the organisation to ransom through financially motivated attacks. A cyber-attack can severely damage an organisation's ability to function, its reputation, and its ability to meet its legal obligations.



The Board is responsible for reviewing and approving a formal cybersecurity strategy. At a minimum, this strategy must address:

- **Identification:** A process for identifying threats, vulnerabilities, and risks specific to the charity.
- **Prevention and Detection:** Measures to reduce the likelihood of security incidents and to detect them in a timely manner when they occur.
- **Incident Handling and Response:** A documented incident response plan that provides a clear roadmap for action during and after a security event.
- **Recovery Planning:** A plan to stabilize and resume critical operations in the immediate aftermath of a security incident.

A critical element of prevention is staff awareness. Human error, often through falling victim to phishing emails, is a leading cause of security breaches. The Board must mandate the implementation of a recurring security awareness training program for all staff and volunteers to build a strong culture of security and mitigate this key risk.

4.4 Business Continuity & Resilience

Effective governance prepares an organisation to withstand disruption. Business Continuity (BC) and Disaster Recovery (DR) planning are essential disciplines for maintaining critical operations in the face of a disruptive event, such as a cyber-attack, power outage, or facility loss. A severe business interruption has the potential to damage a charity's reputation and cause significant harm to its beneficiaries.

Business Continuity & Disaster Recovery

The Distinction: It's not just about Backups (saving data). It's about Recovery (restoring operations).

Governance Check:

- Has the Disaster Recovery Plan (DRP) been TESTED?
- Do we have a specific IT Risk Register?



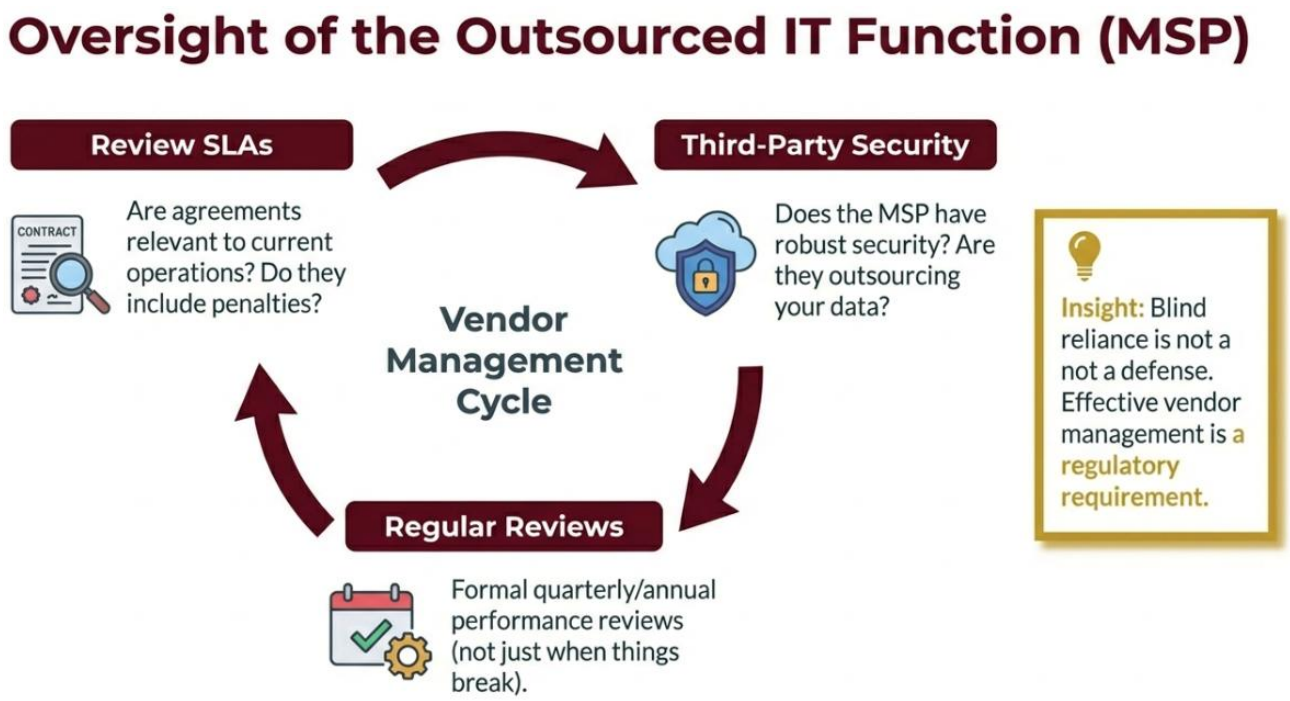
Scenario: If the office burns down or ransomware hits, how long until we can serve our beneficiaries?

The Board should expect the following to be in place:

1. A documented **Business Impact Analysis (BIA)** has been conducted to identify the charity's most critical processes and the resources they depend on.
2. A documented **Disaster Recovery (DR) Plan** is maintained with clear recovery time objectives for critical IT systems.
3. A documented **Business Continuity Plan (BCP)** is maintained that covers a range of plausible scenarios, including the loss of a key IT service provider.
4. All plans are **tested periodically** (at least annually), with the results, key findings, and lessons learned reported back to the Board for review.

4.5 Oversight of Outsourced IT Functions

Many charities rely on external Managed Service Providers (MSPs) for their IT functions. It is critical to understand that **outsourcing the function does not transfer the Board's responsibility for managing the associated risk**. The charity remains fully accountable for the security of its data and the continuity of its services.



Effective oversight of outsourced IT is non-negotiable and must include the following activities:

- **Thorough Due Diligence:** A formal process to evaluate a prospective provider's technical capabilities, financial viability, performance track record, and security controls before any contract is signed.
- **Robust Service Level Agreements (SLAs):** Legally binding contracts that clearly define the scope of service, measurable performance metrics, security requirements, business continuity provisions, and penalties for performance shortfalls.
- **Regular Performance Monitoring:** A formal, recurring process to review the provider's performance against the SLA to ensure they are delivering to the required standard.
- **Formal Exit Strategy:** A documented plan to transition services to another provider or bring them in-house if necessary, ensuring the charity can retrieve all its data securely and efficiently.

4.6 Compliance & Legal Obligations

As stated in Principle 4 of the Charities Governance Code, trustees have a legal duty to find out which laws and regulatory requirements are relevant to their charity and to comply with them. This duty extends to all aspects of IT.

The Regulatory & Legal Imperative

Charities Governance Code

Principle 4 (Exercising Control): Boards must identify and oversee IT-related risks and ensure internal controls are in place.

Principle 6 (Accountability): Transparency for data and resources.



GDPR / Data Protection

Accountability (Article 24), Integrity, and Confidentiality.

Mandatory Breach Notification (72 hours) and Record of Processing Activities (RoPA).



Auditor Obligations (ISA 315)

Auditors are required to identify and assess risks of material misstatement, specifically including Information Technology risks.



Key areas of compliance relevant to IT include:

- Data protection legislation.
- Employment legislation (as it relates to IT usage and remote work).
- Health and safety legislation (as it relates to IT equipment).

By building these pillars into the organisation's governance structure, a charity can move from a reactive to a proactive posture. The next section outlines how to begin this journey.

5.0 A PRACTICAL 12-MONTH ROADMAP TO BETTER GOVERNANCE

Improving IT governance is a journey of continuous improvement, not a one-time project. This actionable, phased plan, adapted from established cybersecurity best practices, provides a lifecycle that any charity can follow to build maturity over time and demonstrate progress to its stakeholders.



Quarter 1: Foundation & Assessment

- **Establish Governance:** Obtain formal support from the Board and SMT. Clearly define roles and responsibilities for IT oversight and establish a cross-functional risk management group that includes all relevant stakeholders.
- **Identify Critical Assets:** Map the charity's core objectives and services to the supporting people, processes, technology, and data infrastructure. Rank these assets by their criticality to the organisation's mission.
- **Understand Threats & Define Risk Appetite:** Analyze potential internal and external threats and vulnerabilities. Formally document and agree upon the level of IT risk the organisation is willing to accept to achieve its objectives.

Quarter 2: Control Implementation

- **Focus on Education & Awareness:** Launch a comprehensive security awareness program for all employees and volunteers, focusing on common threats like phishing and the importance of good security practices.
- **Implement Basic Protections:** Deploy essential technical controls, including boundary firewalls, secure system configurations, regular patch management, anti-malware software, and robust access controls based on the principle of least privilege.
- **Strengthen Outsourcing Oversight:** Review all existing MSP and other IT provider contracts against the criteria outlined in Section 4.5. Develop a clear plan to remediate any identified gaps in due diligence, SLAs, or monitoring.

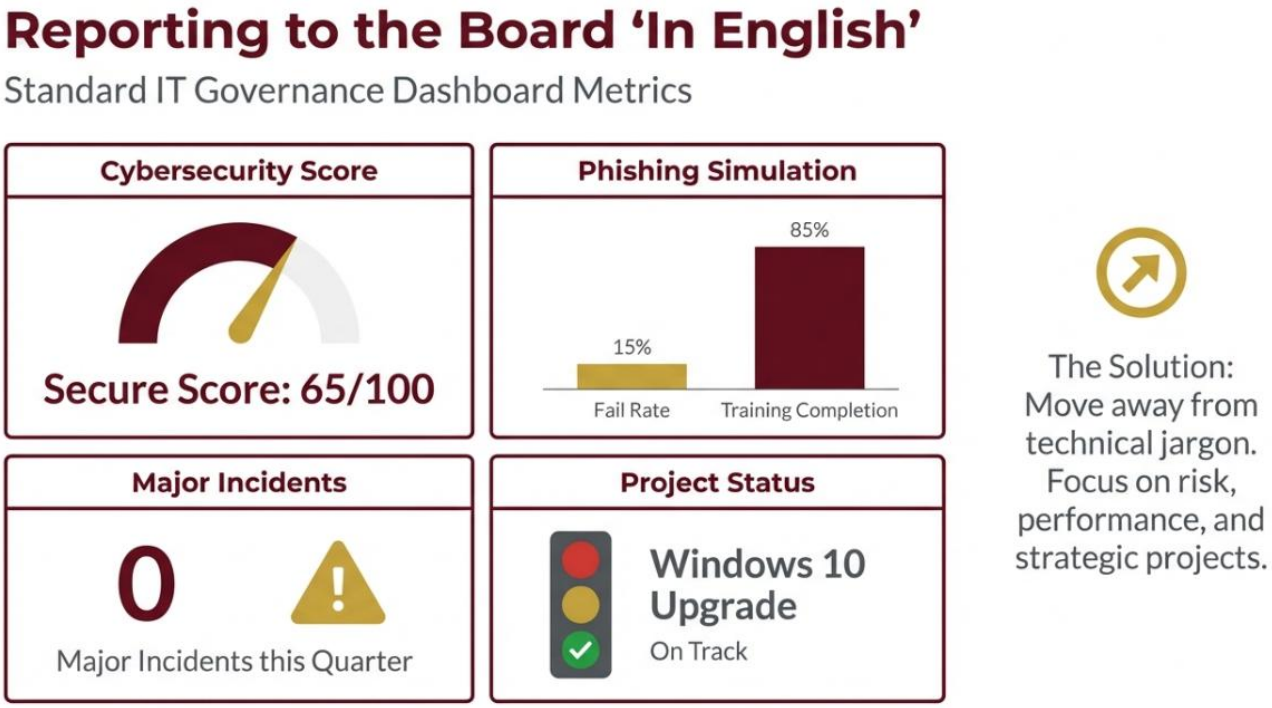
Quarter 3: Detection & Response

- **Establish Detection Capabilities:** Implement security monitoring capabilities to detect suspicious or unusual activity on networks, systems, and applications in a timely manner.
- **Prepare to React:** Create and document a formal Cyber Incident Response Plan. Establish a designated incident response team and ensure they are trained on the plan.
- **Build Resilience:** Develop and document detailed recovery plans and comprehensive backup strategies for all critical systems and data, ensuring they align with the Business Impact Analysis.

Quarter 4: Testing & Improvement

- **Challenge & Test:** Conduct a cyber incident simulation exercise to test the incident response plan and the leadership team's ability to manage a crisis. Test backup restoration capabilities to verify their effectiveness.
- **Review & Mature:** Reflect on the progress made across all areas of the program. Identify areas for ongoing improvement and repeat the risk assessment process to account for changes in the threat landscape.
- **Report to the Board:** Present a formal report to the Board on the progress achieved during the 12-month cycle, the current risk posture, and the strategic plan for the next cycle of improvement.

This structured approach provides a clear path from assessment to maturity, setting the stage for the final key recommendations.



6.0 SUMMARY AND KEY RECOMMENDATIONS

Good IT governance is an essential and ongoing responsibility of the Board and Senior Management. It is not an optional extra or a purely technical concern; it is a core component of effective leadership, critical for protecting a charity's operations, reputation, and, most importantly, its beneficiaries. Moving from a reactive to a proactive stance on IT oversight is fundamental to modern risk management.

For trustees and SMTs seeking to enhance their governance posture, the following actions represent the most critical first steps:

1. **Make IT a Standing Board Agenda Item:** Elevate IT from a background operational concern to a recurring strategic topic for discussion, review, and challenge at the Board level. This ensures consistent visibility and accountability.
2. **Approve and Resource an IT Strategy:** Ensure a formal, documented IT strategy exists that is explicitly aligned with the organisation's overarching strategic plan. The Board must approve this strategy and commit the necessary resources to its execution.
3. **Demand Comprehensible Reporting:** Insist on receiving IT and risk reports that are clear, concise, and focused on business impact and risk posture, not just technical metrics. Reports must be in a format that enables informed decision-making.
4. **Actively Manage Your MSP:** Treat your IT provider as a critical strategic partner, not just a vendor. Their performance must be actively and formally monitored against a robust and comprehensive Service Level Agreement (SLA).
5. **Champion a Culture of Security:** Lead by example in promoting and participating in security awareness training. A strong security culture starts at the top and is one of the most effective defences against cyber threats.

By embracing these principles, a charity will not only mitigate significant risks but will also be better positioned to leverage technology as a powerful tool for innovation and efficiency. Good governance transforms IT from a potential liability into a strategic asset that can more effectively advance the organisation's charitable purpose.



APPENDIX 1: SAMPLE IT RISK APPETITE STATEMENT

IT Risk Appetite Statement

Overall Risk Rating: Low (Minimalist) Score Target: < 10

Statement of Philosophy

The Charity has a **minimalist** appetite for Information Technology risk. This reflects our priority to safeguard charity funds and critical services. We are willing to accept only a low level of uncertainty in our IT environment and require strong internal control processes to mitigate threats.

While we recognise that new technologies create opportunities, our appetite for risks arising from ongoing development is low. We prioritise the maintenance of a secure and stable environment over the rapid adoption of unproven technologies.

Specific Risk Areas & Appetite

Risk Area	Appetite Level	Description & Expectations
Cybersecurity	**Minimalist**	We have a minimalist appetite for external malicious attacks. We require robust technology solutions (firewalls, endpoint security) and strong internal controls to protect our assets and data.
System Availability	**Minimalist**	We have a minimalist appetite for system downtime that impacts critical business processes. Maximum recovery times must be defined in the Business Continuity Plan and tested annually.
Data Integrity	**Minimalist**	We have no appetite for the deliberate misuse of information. We require ensuring information is relevant, accurate, timely, and managed in strict accordance with legislative requirements (e.g., GDPR).
Outsourcing	**Minimalist**	We will only outsource to experienced parties where capability is higher than internal resources. All third-party providers must meet strict Service Level Agreements (SLAs) regarding security and uptime.

Key Risk Indicators (KRIs) & Tolerances

To ensure we remain within our risk appetite, the Board monitors the following metrics. Breaching these "Triggers" requires immediate reporting to the Audit & Risk Committee.

Indicator	Measure	Tolerance Trigger (Red Flag)
Cyber Incidents	Volume of security alerts generated by firewalls/IDS.	**>20% increase** above baseline average.
System Downtime	Actual downtime of operational IT systems per quarter.	**>5%** of total operating time.
IT Budget	Variance between Actual IT Costs and Projected Budget.	**>5%** variance.
Data Incidents	Number of Data Protection incidents or "near misses."	**>1** event per month.

APPENDIX 2: SAMPLE QUESTIONS FOR TRUSTEES TO DEMONSTRATE IT OVERSIGHT

These sample questions will help Trustees to challenge content, hold parties to account, and discharge their legal duties.

1. Strategy and Alignment

• **To SMT:** "Does our IT Strategy exist as a standalone document, and can you demonstrate how it explicitly supports our charity's mission and strategic objectives for the next 12-24 months?"

◦ *Context:* IT Governance is defined as the framework ensuring IT "supports and enables the achievement of strategic goals". There is a specific risk of "Board-Level Detachment from IT Strategy" where IT is treated as a silo rather than a strategic enabler.

• **To SMT:** "Are we budgeting for strategic IT investment, or are maintenance costs crowding out our ability to adopt new technologies?"

◦ *Context:* A reactive strategy ("We'll Use It Until It Dies") is no longer viable and leaves charities vulnerable. Boards must ensure IT is viewed as a "strategic necessity — not a luxury".

• **To MSP:** "Regarding 'Windows 10 Cessation' in October 2025, do we have a budgeted plan to replace or upgrade non-compatible devices before security updates stop?"

◦ *Context:* Running Windows 10 beyond 2025 poses security risks and may be seen as negligence under GDPR Article 32.

2. Risk Management & Appetite

• **To SMT:** "Is our IT Risk Register 'forward-looking' regarding emerging threats, or is it purely reactive based on past incidents?"

◦ *Context:* A common weakness is risk identification being "backward rather than forward looking". The register must address risks like "Severe Cyber Attacks" and "Ineffective Data Management",.

• **To SMT:** "Can you confirm that our current residual risk scores fall within the 'Minimalist' (or agreed) risk appetite we set? If any risk is 'High' (score >20), what is the specific remediation plan?"

◦ *Context:* The board must define risk appetite (e.g., Minimalist/Low). Risks exceeding this capacity must be reported immediately with a plan to bring them back within tolerance,.

• **To SMT/MSP:** "How does our current 'Microsoft Secure Score' compare to the non-profit sector average, and what specific actions are we taking to reach the target of 80%?"

◦ *Context:* The Secure Score is a plain English metric (e.g., 47.23%) that allows the board to track improvement over time without needing deep technical knowledge.

3. Cybersecurity & Incident Response

• **To SMT:** "When was the last time we conducted a phishing simulation exercise for staff, and what were the failure rates?"

◦ *Context:* Phishing is the most likely threat. The HSE cyber-attack began with a phishing email. "Underinvestment in Staff Cyber Awareness" is a top risk.

• **To MSP:** "Can you confirm that Multi-Factor Authentication (MFA) is enforced on **all** remote access and privileged (admin) accounts, without exception?"

◦ *Context:* MFA is a critical control. The sources note that robust safeguards must include strong authentication and access controls.

• **To SMT:** "We have a Cyber Incident Response Plan (CIRP), but when was it last tested? Who acts as the 'First Responder,' and do they know their role?"

◦ *Context:* Having a plan is not enough; it must be "reviewed and tested at regular intervals". The plan needs to define roles, including who communicates with regulators (DPC).

4. Outsourcing & MSP Oversight

• **To SMT:** "Have we reviewed the Business Continuity Plan (BCP) of our MSP? How do we know *they* can recover if they are attacked?"

◦ *Context:* You cannot assume the provider is safe. You must ensure you are not "left exposed by the actions or inaction of a material service provider".

• **To MSP:** "Can you provide a report on your performance against our Service Level Agreement (SLA) this quarter? Have there been any breaches in response times or uptime?"

◦ *Context:* SLAs must include measurable performance metrics and remedies for shortfalls. There is a risk of "Ineffective IT Service Provider" if SLAs are weak or penalties are not enforced.

• **To SMT:** "Do we have a documented 'Exit Strategy' if we need to leave this MSP or if they fail? Can we retrieve our data easily?"

◦ *Context:* Firms must maintain an exit management strategy to reduce disruption risks if services are unexpectedly withdrawn.

5. Business Continuity & Resilience

• **To MSP:** "We know backups are running, but when was the last time we performed a 'restore test' to prove we can actually get the data back and run the business?"

◦ *Context:* A common finding is that companies fail to perform "regular backup and restore tests to verify the restore capabilities".

• **To SMT:** "What is our 'Impact Tolerance' for a system outage? If our membership database goes down, how long can we operate manually before it threatens our viability?"

◦ *Context:* The board must approve "impact tolerances" (maximum acceptable disruption). Testing should prove the firm can stay within these limits.

6. Asset & Data Management

• **To SMT:** "Do we have a fully up-to-date IT Asset Register that includes all hardware and software? How do we track devices used by remote workers?"

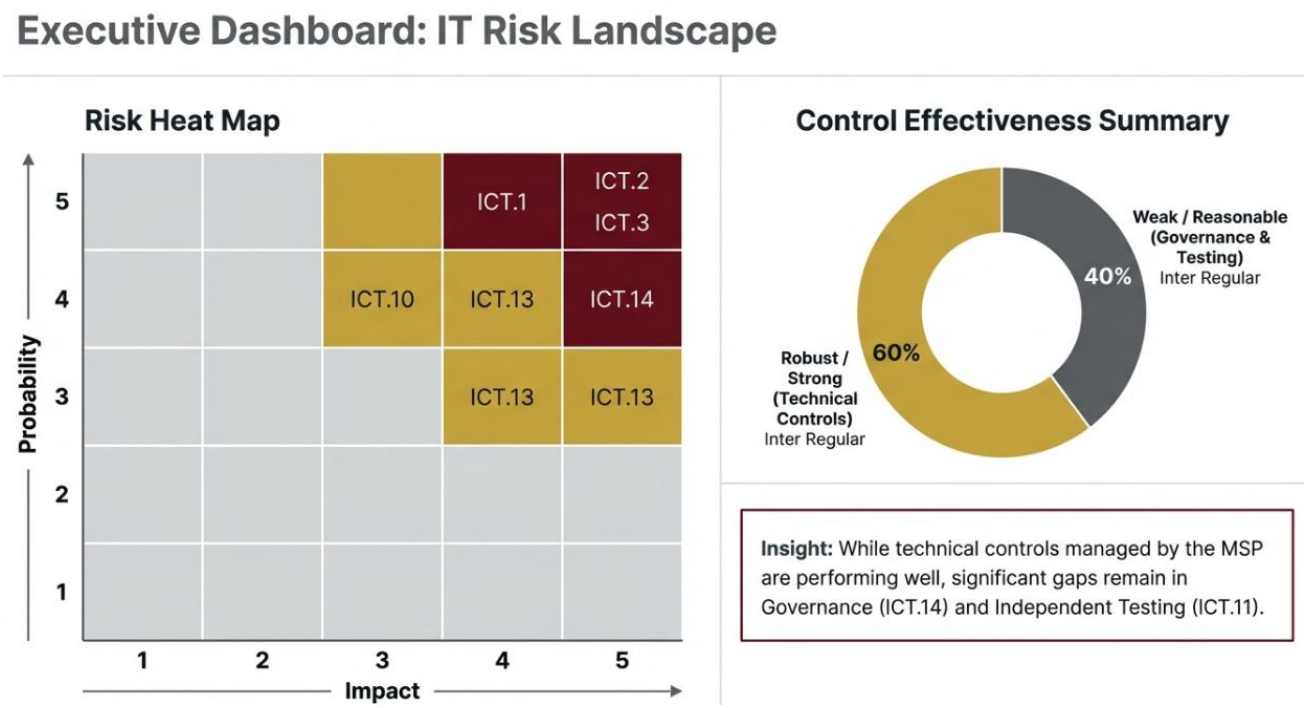
◦ *Context:* You cannot protect what you don't know. A register is essential for GDPR compliance and budgeting. "Shadow IT" (personal devices) carries significant risks like data loss and lack of encryption.

• **To MSP:** "Where exactly is our data stored (geographically), and is it encrypted 'at rest' and 'in transit'?"

◦ *Context:* Contracts with cloud providers must specify the location of data storage. Data should be encrypted to ensure confidentiality.

APPENDIX 3: SAMPLE IT RISK REGISTER ASSESSMENT TEMPLATE





Pillar 1: Cybersecurity & External Threats

STATUS: ROBUST / STRONG

- **Risks Covered:** ICT.1 (Severe Attacks), ICT.4 (Phishing), ICT.5 (End Point), ICT.9 (Server Room).
- **Threat Monitoring:** MSP uses MS Defender to monitor threat scores; all endpoints protected.
- **Infrastructure:** Migration to M365/Azure; data stored in Microsoft Data Centers; no physical servers on-site.
- **Configuration:** USB ports disabled; unauthorized programs blocked by MSP; active patching cycles.

WDA Auditor's Voice

Finding: We discussed controls with the CEO and senior management. There has been no instance of cyberattacks reported. Due to the migration to Azure and MSP oversight, we are satisfied there are strong controls in place.

Pillar 2: Data Integrity & Operations

STATUS: STRONG / REASONABLE

- **Risks Covered:** ICT.2 (Data Mgmt), ICT.3 (Internal Misuse), ICT.6 (Backups), ICT.7 (Website/Email).
- **Backups:** Automated daily backups in Azure with failover capabilities.
- **Training:** Staff receive annual cybersecurity and data protection training.
- **Access Control:** 'Principle of least privilege' applied; access rights reviewed by CEO.

WDA Auditor's Voice

Gap Identification: While an Internet usage policy exists, the company does not actively monitor all daily activity of its staff, relying heavily on trust. Additionally, access to social networking sites is not technically restricted, increasing the risk of policy non-adherence (ICT.12).

Pillar 3: IT Governance & Strategy

STATUS: WEAK / REQUIRES IMPROVEMENT

- **Risks Covered:** ICT.14 (Governance Framework), ICT.16 (IT Strategy), ICT.8 (Change Mgmt).
- **Governance Void:** No IT Risk Committee established. No documented IT Risk Register existed prior to this review.
- **Board Oversight:** IT knowledge at the Board level is challenged. Reporting is not conducted on a quarterly basis.
- **Strategic Gap:** No documented IT Strategy exists outside of the general strategic plan.

WDA Auditor's Voice

Critical Finding: The size of the CLG precludes employing an in-house IT expert, leading to total reliance on the outsourced MSP. However, IT Governance at the Board level is weak There is insufficient expertise to challenge the MSP or oversee the risk framework effectively.

Pillar 4: Resiliency & Third-Party Management

STATUS: REASONABLE / WEAK

- **Risks Covered:** ICT.11 (Resiliency/Continuity), ICT.13 (Service Provider), ICT.17 (Testing).
- **The Reliance Issue:** The entity is heavily dependent on the MSP. While the MSP is reliable, independent oversight is weak.
- **Testing Gap:** Lack of 'Scenario Planning' or 'End-to-End process testing' (ICT.11).

WDA Auditor's Voice

Finding: The Company is weak on running BCP tests and relies entirely on the third party. We recommend a formal request be made to all material outsourced service providers for a copy of their BCP to ensure the company is not left exposed.

WDA Independent Gap Analysis

Strengths (Technical & Operational)

- **Environment:** Full migration to M365/Azure eliminates physical hardware risks.
- **Defense:** MSP actively blocks ports, enforces patching (forced restarts), and uses phishing monitoring software.
- **Track Record:** No history of breaches; strong asset lifecycle management (destruction certificates provided).

Critical Gaps (Governance & Oversight)

- **Oversight:** Lack of IT expertise on the Board to challenge the MSP.
- **Verification:** No independent testing of the Business Continuity Plan (BCP) or Disaster Recovery scenarios.
- **Documentation:** Absence of a specific IT Strategy document to guide investment in emerging technologies.

Strategic Roadmap & Remediation

Immediate (0-3 Months)

- **Action:** Establish an IT Risk Committee or recruit a Director with IT expertise.
- **Goal:** Address Risk ICT.14 (Ineffective Governance).

Short Term (3-6 Months)

- **Action:** Conduct a formalized BCP/Scenario Test independent of the MSP. Request MSP's own BCP for review.
- **Goal:** Address Risk ICT.11 (Resiliency) and ICT.17 (Testing).

Ongoing

- **Action:** Develop a formal IT Strategy document including cost-benefit analysis for new technologies.
- **Goal:** Address Risk ICT.16 (Ineffective IT Strategy).