



Collection: **Irreplaceable** in the AI Era™

"Because leadership begins with you"

This is not just another ebook.

It's a practical guide for leaders who—amid the relentless advance of technology and artificial intelligence—seek to ensure that their leadership, decisions, and results remain relevant and sustainable.

It was conceived and written from a place of deep conviction—combining strategic clarity with the genuine love for positive impact, the personal power that comes from lived experience, and the essence of leading with integrity. Every concept, framework, and tool included here has been chosen with a single purpose: to deliver real value that can tangibly transform the way you lead and generate results.

Experience shows that most failed transformations don't fall short because of technical limitations, but because of invisible factors that silently erode performance: internal resistance, cultural misalignment, loss of strategic focus, or lack of team commitment. These rarely appear in the metrics—yet they determine the success or failure of any initiative.

In this guide, you'll find actionable tools and frameworks to help you:

- Identify and anticipate risks that can slow or derail your strategy.
- Protect and strengthen your leadership capacity in high-disruption environments.
- Use technology—including AI—as a multiplier of results, not as a replacement.
- Stay competitive without compromising your team's cohesion or your organization's future.

This resource is available in PDF format for quick reference. If you prefer the editable version, you'll find a link to the download center at the end, where you can get it in Word format and adapt it to your needs. A new ebook will be added to the collection every week—until all 25 are complete. Simply visit the download center to see what's new each week.

If these words have reached you, it's likely not by chance. You are in the right position, at the right time, and in the right circumstances for this information to make a real difference. And as you put it into practice, you may discover it could also spark transformation in others.

Because in today's era, real value lies not just in the technology you use—but in your ability to lead with vision, precision, and purpose.

2. Central Theme of the Ebook

Securing Technological Evolution: how to systematically keep your technology landscape relevant, safe and aligned with your strategy, instead of reacting only when systems fail or vendors discontinue products.

We will work through five key levers:

1. Periodic technology audits.
 2. Replacement of obsolete systems.
 3. Integration of new tools.
 4. Continuous training in technology.
 5. Monitoring of disruptive trends.
-

3. Initial Sections

3.1. Why technological evolution matters in a transforming world

Without a deliberate approach to technological evolution, organizations tend to oscillate between two extremes:

- **Over-stability:** legacy systems, rigid processes, outdated architectures, growing technical debt and rising risk.
- **Chaotic experimentation:** uncoordinated pilots, tool proliferation, duplicated data, unclear ownership and security gaps.

Both extremes are expensive. Both erode trust—internally and with customers.

A disciplined, human-centered approach to technological evolution enables you to:

- Manage risk proactively.
- Improve efficiency and resilience.
- Open space for innovation without losing control.
- Attract and retain talent who want to work with modern tools and architectures.

3.2. Purpose of this guide

This guide aims to help you:

1. **Clarify** what “ensuring technological evolution” means in your context.
2. **Equip** you with tools to audit, prioritize and modernize your technology stack.
3. **Illustrate** through “caso hipotético” scenarios how other organizations could deal with similar challenges.

4. **Provide** templates to design audits, replacement plans, integration roadmaps and training programs.
5. **Inspire** you to create a governance rhythm where technology decisions are transparent, data-informed and aligned with human needs.

3.3. How to read with your team

Consider reading this ebook with a cross-functional group that includes technology, operations, risk, finance and business leaders.

- Use each subtopic as a **chapter for a working session**.
- Fill in the tables live, using the example rows as a guide.
- Capture decisions and turn them into 30–60–90 day plans.
- Revisit the KPIs and checklists in your monthly or quarterly business reviews.

The more diverse the team, the richer the discussion and the more robust the decisions.

4. Core Module – Development of the Topic

Subtopic 1 – Periodic Technology Audits

4.1.1. Definition

A technology audit is a structured review of your systems, infrastructure, data, processes and governance practices to assess their alignment with business objectives, risks and standards. When done periodically and with a cross-functional lens, technology audits help you see beyond day-to-day firefighting and detect issues before they become crises.

An audit is not a hunt for culprits; it is a disciplined way to ask:

- What still serves us well?
- What creates friction, risk or unnecessary cost?
- Where are we missing opportunities to use technology better?

4.1.2. Practical framework

A robust audit process can be organized into five phases:

1. **Scope and objectives**
 - o Decide which domains you will review: infrastructure, applications, data, cybersecurity, vendors, processes, governance.
 - o Clarify why you are auditing: regulatory compliance, cost optimization, risk management, readiness for new initiatives, or all of the above.
2. **Information gathering**
 - o Collect inventories of systems, interfaces, contracts and documentation.
 - o Map data flows and dependencies.
 - o Interview key users and support teams to capture pain points.
3. **Assessment and rating**
 - o Evaluate each asset along dimensions such as stability, performance, security, scalability, maintainability, and business value.
 - o Use standardized scales (for example, 1–5) to enable comparison.
4. **Prioritization and recommendations**
 - o Identify quick wins, high-risk items and strategic opportunities.
 - o Propose actions: keep, improve, migrate, replace, consolidate or retire.
5. **Communication and follow-up**
 - o Present findings in clear language, avoiding overly technical jargon.
 - o Assign owners and deadlines.
 - o Integrate audit results into budget planning and project portfolio management.

JavierSimpleMan™

Collection: **Irreplaceable** in the AI Era™ — "*Because leadership begins with you*"

4.1.3. Caso hipotético

Caso hipotético: A regional retail company decides to run a technology audit after a series of outages affecting its e-commerce platform.

- The audit discovers more than 180 applications in use, with multiple duplications and unsupported versions of critical software.
- Legacy systems handling inventory are poorly documented and depend on a few individuals.
- Several integrations use manual file transfers without encryption.

Using a simple rating system (Business Value, Risk, Technical Health), the team classifies systems and identifies 12 high-risk assets that require immediate attention. Within six months, they retire three low-value applications, reinforce security controls in critical integrations and design a roadmap to modernize the inventory system. Outages decrease significantly and IT and business leaders share a clearer view of priorities.

4.1.4. Exercise – Designing Your Technology Audit

Objective: Define the scope, criteria and cadence of a periodic technology audit for your organization.

- **Roles involved:**
 - Executive sponsor (CIO/CTO or equivalent).
 - Enterprise architect or technology strategy lead.
 - Representatives from security, operations and key business units.
- **Inputs:**
 - Current system inventory (even if incomplete).
 - Recent incidents, audit reports or regulatory requirements.
 - Strategic roadmap and budget cycles.
- **Suggested time:** 2 sessions of 90 minutes.
- **Steps:**
 - Agree on the primary objectives of the audit (max. three).
 - Decide which domains to include in the first cycle and which to leave for later.
 - Select assessment criteria and rating scales.
 - Define roles, responsibilities and timeline.
 - Capture the plan in the Technology Audit Map below.
- **Deliverables:**
 - Technology Audit Map completed.
 - Draft communication to stakeholders explaining purpose and timeline.

4.1.5. Template – Technology Audit Map

Domain / System Group	Objective of Review	Main Criteria (examples)	Frequency	Owner	Next Audit Date	Notes
Core transactional systems (ERP, billing)	Assess risk and modernization needs	Availability, support status, security, integration complexity, business criticality	Annual	CIO	15/09	Use external specialist for security review

4.1.6. Checklist & KPIs

Checklist – Periodic Technology Audits

- ☐ Objectives and scope of the audit are clearly defined.
- ☐ There is a documented inventory of systems and integrations.
- ☐ Assessment criteria are consistent across domains.
- ☐ Audit results are translated into concrete actions with owners.
- ☐ Audit outcomes feed into budget and portfolio decisions.

Suggested KPIs

- Percentage of systems covered by the audit in the last 12 months.
 - Number of high-risk findings addressed within agreed timeframes.
 - Reduction in critical incidents or outages after audit-driven actions.
 - Percentage of systems with up-to-date documentation.
-

Subtopic 2 – Replacement of Obsolete Systems

4.2.1. Definition

Obsolete systems are those that no longer meet business needs, security requirements, performance expectations or vendor support standards. They often become “black boxes” that everyone depends on but nobody wants to touch.

Replacing obsolete systems is not only a technical project; it is an organizational change journey. It involves processes, data, interfaces, habits and sometimes identity (“we have always done it this way”).

4.2.2. Practical framework

1. **Identify obsolescence criteria**
 - o End-of-life vendor status.
 - o Incompatibility with current security requirements.
 - o High frequency of incidents.
 - o Inability to support new business models or regulatory needs.
2. **Assess business impact**
 - o What processes depend on the system?
 - o What risks arise if it fails?
 - o What opportunities are blocked by its limitations?
3. **Define replacement strategy**
 - o **Lift-and-shift:** migrate to modern infrastructure with minimal changes.
 - o **Refactor:** restructure and optimize existing code.
 - o **Replatform:** move to a different platform (for example, cloud-based).
 - o **Rebuild or replace:** build a new system or adopt a SaaS solution.
4. **Plan transition carefully**
 - o Data migration and cleansing.
 - o Parallel runs and fallback options.
 - o Training and communication to users.
5. **Retire the old system**
 - o Archive data according to regulatory requirements.
 - o Decommission infrastructure and licenses.
 - o Capture lessons learned.

4.2.3. Caso hipotético

Caso hipotético: A logistics company relies on a 15-year-old on-premise application to manage routes and fleet data. The vendor announces end-of-support and the system cannot integrate with new mobile apps used by drivers.

- The audit classifies the system as high business value and high risk.
- After evaluating alternatives, the company chooses a SaaS transportation management system.

- They plan a phased rollout: first for one region, then others. Historical data is migrated gradually, and critical reports are recreated with better visualization tools.
- During migration, they keep read-only access to the old system as a safety net. After six months, they fully decommission it and reduce infrastructure and maintenance costs significantly.

4.2.4. Exercise – Obsolete Systems Replacement Portfolio

Objective: Build a portfolio of obsolete systems and define replacement priorities.

- **Roles involved:**
 - o CIO/CTO.
 - o Enterprise architect.
 - o Business owners of key systems.
 - o Risk/compliance representative.
- **Inputs:**
 - o Audit findings (if available).
 - o Information on vendor support, incidents and user complaints.
- **Suggested time:** 2–3 hours.
- **Steps:**
 - o List systems that meet one or more obsolescence criteria.
 - o For each, rate business criticality and risk level.
 - o Define preferred replacement strategy.
 - o Estimate effort and timeline.
 - o Prioritize using the impact × effort rubric from the global tools section.
- **Deliverables:**
 - o Obsolete Systems Replacement Portfolio table.

4.2.5. Template – Obsolete Systems Replacement Portfolio

System	Business Criticality (H/M/L)	Risk Level (H/M/L)	Main Pain Points	Preferred Strategy (lift-and-shift / replatform / replace)	Estimated Effort (1–5)	Target Date	Owner
Legacy Fleet Management App	High	High	No mobile integration, vendor end-of-support, frequent downtime	Replace with SaaS TMS	4	30/06 next year	Head of Operations & CIO

4.2.6. Checklist & KPIs

Checklist – Replacement of Obsolete Systems

- ☐ Obsolescence criteria are defined and communicated.
- ☐ The list of obsolete systems is updated at least annually.
- ☐ Replacement strategies are aligned with business priorities and architecture principles.
- ☐ Transition plans include data, process and people dimensions.
- ☐ Old systems are formally decommissioned and not kept running “just in case” without justification.

Suggested KPIs

- Percentage of systems classified as obsolete that have an approved replacement plan.
 - Number of critical incidents related to obsolete systems.
 - Reduction in maintenance costs after replacement.
 - Percentage of users trained before go-live of new systems.
-

Subtopic 3 – Integration of New Tools

4.3.1. Definition

Integrating new tools means connecting new applications, platforms or services with your existing technology landscape so that data flows securely, processes remain coherent and users have a consistent experience.

In many organizations, lack of integration leads to silos, double data entry, inconsistent reports and security exposures. A thoughtful integration strategy turns new tools from isolated experiments into real capabilities.

4.3.2. Practical framework

1. **Start with the problem, not the tool**
 - o Clarify which business problem or opportunity the new tool is meant to address.
 - o Define success criteria before selecting vendors.
2. **Evaluate integration requirements early**
 - o What data needs to flow in and out?
 - o What systems will it interact with (CRM, ERP, data warehouse, identity provider)?
 - o What regulatory or security constraints apply?
3. **Choose integration patterns**
 - o APIs and microservices.
 - o Event-driven architectures.
 - o ETL/ELT pipelines or data replication.
 - o Simple batch files when appropriate (but with security controls).
4. **Design for resilience and observability**
 - o Error handling, retries and alerting.
 - o Monitoring dashboards for key interfaces.
5. **Govern tool adoption**
 - o Avoid proliferation of overlapping solutions.
 - o Define who approves new tools and under what criteria.
 - o Maintain an updated integration catalog.

4.3.3. Caso hipotético

Caso hipotético: A bank wants to introduce a new AI-powered customer support chatbot.

- The business objective is to reduce average response time and increase 24/7 availability.
- The integration team identifies necessary connections: core banking for balances, CRM for customer context, authentication systems and logging for compliance.
- They design APIs to expose only necessary data, with strict access controls.

- The chatbot is first integrated in a sandbox with synthetic data, then in a pilot with a limited customer segment.
- Monitoring shows that customer satisfaction improves and no security incidents occur; the solution is then scaled.

4.3.4. Exercise – New Tool Integration Canvas

Objective: Define the integration approach for a new tool you plan to adopt.

- **Roles involved:**
 - o Product owner or business sponsor.
 - o Solution architect.
 - o Security officer.
 - o Data owner(s).
- **Inputs:**
 - o Business case or initial idea.
 - o Basic documentation from potential vendors.
- **Suggested time:** 90 minutes.
- **Steps:**
 - o Describe the business goal and key use cases.
 - o List systems that must interact with the new tool.
 - o Define required data flows and their sensitivity.
 - o Choose preferred integration patterns.
 - o Identify risks and mitigation measures.
- **Deliverables:**
 - o New Tool Integration Canvas table.

4.3.5. Template – New Tool Integration Canvas

Element	Description	Example / Notes
Business Goal	What we want to achieve	Reduce average customer support response time by 30%
Systems Involved	Main systems that must connect	CRM, core banking, identity provider, logging platform
Data Flows	Key data exchanged	Customer profile, product holdings, conversation logs
Integration Pattern	Chosen approach	REST APIs for real-time queries, event bus for notifications
Risks & Mitigation	Main risks and how to manage them	Data privacy → strict access scopes; performance → caching layer
Element	Description	Example / Notes

4.3.6. Checklist & KPIs

Checklist – Integration of New Tools

- ☐ Each new tool has a clearly defined business goal.
- ☐ Integration requirements are documented before signing contracts.
- ☐ Data flows are mapped, including security and privacy considerations.
- ☐ Monitoring is set up to detect integration failures quickly.
- ☐ There is a governance process to avoid redundant tools.

Suggested KPIs

- Percentage of new tools with documented integration designs before implementation.
 - Number of integration-related incidents in the last 12 months.
 - Average time to resolve integration failures.
 - Reduction in manual data entry between systems.
-

Subtopic 4 – Continuous Training in Technology

4.4.1. Definition

Continuous training in technology means maintaining a sustained learning rhythm so that people stay up to date with tools, platforms and practices relevant to their roles. It goes beyond sporadic courses and focuses on building a culture where learning is part of daily work.

This includes not only technical teams but also business leaders, who must understand the implications of AI, data governance, cybersecurity and digital products on strategy and risk.

4.4.2. Practical framework

1. **Define learning priorities by role**
 - o For example: cloud fundamentals, cybersecurity hygiene, data literacy, AI basics, DevOps practices, product management.
2. **Create a blended learning ecosystem**
 - o Online courses, internal academies, communities of practice, tech talks, hackathons, brown-bag sessions.
3. **Integrate learning into performance management**
 - o Include learning objectives in individual plans.
 - o Recognize and reward knowledge sharing.
4. **Measure and adapt**
 - o Track participation, completion, learner feedback and impact on work quality.
 - o Use metrics to refine content and formats.

4.4.3. Caso hipotético

Caso hipotético: A utilities company launches several cloud and analytics initiatives but realizes that many managers still think in terms of on-premise systems and manual reports.

- The CIO and CHRO co-design a “Digital Fluency Program” for 120 managers.
- The program mixes short videos, live sessions, case discussions and hands-on labs with real company data.
- Managers must complete a small project applying what they learned (for example, redesigning a report as an interactive dashboard).
- After the first cohort, surveys show higher confidence in discussing technology strategy, and project prioritization conversations become more evidence-based.

4.4.4. Exercise – Technology Learning Map

Objective: Map key technology learning needs and define initial programs.

- **Roles involved:**
 - HR / Learning & Development lead.
 - CIO/CTO or technology leaders.
 - Representatives from critical business areas.
- **Inputs:**
 - Existing training catalog.
 - Current and planned technology initiatives.
- **Suggested time:** 2 hours.
- **Steps:**
 - List key role families (for example, developers, analysts, frontline managers, executives).
 - For each, identify priority topics and current capability level (1–5).
 - Decide which topics need structured programs in the next 6–12 months.
 - Assign owners, formats and timing.
- **Deliverables:**
 - Technology Learning Map table.

4.4.5. Template – Technology Learning Map

Role Family	Priority Topic	Current Level (1–5)	Target Level (1–5)	Learning Format (course, lab, mentoring, etc.)	Owner	Start Date	Notes
Mid-level managers	Data literacy and dashboard interpretation	2	4	Blended program (videos + workshops with real data)	L&D Lead	01/10	Align with Q4 planning cycle

4.4.6. Checklist & KPIs

Checklist – Continuous Training in Technology

- ☐ Technology learning needs are mapped for key roles.
- ☐ There is a recurring learning calendar, not just isolated courses.
- ☐ Managers actively support and participate in learning initiatives.
- ☐ Learning outcomes are linked to real projects and business metrics.

- ☐ Communities of practice or peer-learning spaces exist.

Suggested KPIs

- Percentage of employees who completed at least one relevant technology training in the last 12 months.
 - Improvement in self-reported confidence in using key tools.
 - Number of internal projects led by graduates of specific programs.
 - Reduction in errors or incidents linked to lack of knowledge.
-

Subtopic 5 – Monitoring Disruptive Trends

4.5.1. Definition

Monitoring disruptive trends means systematically scanning the technological environment to identify emerging tools, platforms, business models and regulations that could significantly impact your organization—positively or negatively.

It is not about chasing every novelty; it is about building a radar that helps you decide when to observe, when to experiment and when to invest.

4.5.2. Practical framework

1. **Define thematic lenses**
 - o For example: AI and automation, cybersecurity, cloud and edge computing, industry-specific technologies, regulation, sustainability tech.
2. **Assign sensing roles**
 - o Identify individuals or teams who will monitor specific topics.
 - o Include both technology and business perspectives.
3. **Establish information sources**
 - o Conferences, vendor briefings, open communities, academic publications, startup ecosystems, regulatory updates.
4. **Create a simple reporting rhythm**
 - o Monthly or quarterly “technology radar” sessions.
 - o Short summaries: what is emerging, why it matters, potential next steps.
5. **Connect sensing with experimentation**
 - o Link the radar to a small innovation budget.
 - o Design structured pilots with clear hypotheses and success criteria.

4.5.3. Caso hipotético

Caso hipotético: A health insurance company wants to anticipate how AI and remote monitoring could change risk models and customer interactions.

- The CIO creates a small “Tech Radar” team with members from IT, data science, medical affairs and product.
- They select four focus themes: AI diagnostics, wearables, privacy-enhancing technologies and digital health regulation.
- Every quarter, the team presents a radar map with technologies rated by maturity and potential impact.
- The board approves two small pilots per year, such as testing AI-supported triage tools under strict ethical guidelines.

Over time, the company becomes more proactive in partnerships and product design, and regulators see it as a constructive actor.

4.5.4. Exercise – Building Your Technology Radar

Objective: Define how your organization will monitor disruptive trends and turn insights into action.

- **Roles involved:**
 - CIO/CTO or innovation head.
 - Representatives from strategy, risk, and key business lines.
- **Inputs:**
 - Strategic plan and risk register.
 - Existing innovation or R&D initiatives.
- **Suggested time:** 2 sessions of 90 minutes.
- **Steps:**
 - Select 4–6 thematic lenses relevant to your context.
 - Assign owners for each lens.
 - Define information sources and cadence.
 - Design a simple radar report format.
 - Agree on how radar insights will feed into pilots and investment decisions.
- **Deliverables:**
 - Technology Radar Charter table.

4.5.5. Template – Technology Radar Charter

Theme	Owner	Main Information Sources	Reporting Frequency	Example Output	Next Review Date
AI & Automation in Operations	Head of Data & AI	Industry reports, vendor roadmaps, academic labs, startup demos	Quarterly	Radar quadrant with top 10 use cases by impact vs. maturity	15/11

4.5.6. Checklist & KPIs

Checklist – Monitoring Disruptive Trends

- ☐ There is a defined structure for monitoring technology trends.
- ☐ Specific individuals or teams are accountable for sensing and reporting.
- ☐ Trend insights are discussed in strategic and portfolio meetings.
- ☐ Experiments are designed with clear hypotheses and metrics.
- ☐ Learnings from pilots are captured and shared.

Suggested KPIs

- Number of radar reports produced per year.
 - Percentage of radar insights that lead to pilots or studies.
 - Time from identifying a relevant trend to launching a pilot.
 - Share of budget allocated to experimentation with emerging technologies.
-

5. Global Templates and Tools

The following tools support all five subtopics and help you translate insights into coordinated action.

5.1. Impact × Effort Prioritization Rubric

Use this rubric to prioritize technology evolution initiatives (audits, replacements, integrations, training programs, pilots).

Initiative	Impact (1–5)	Effort (1–5)	Priority (High/Med/Low)	Owner	Next Milestone	Date
Replace legacy inventory system	5	4	High	CIO	Business case approved	30/10

5.2. RACI Matrix for Technology Evolution Program

Activity	R (Responsible)	A (Accountable)	C (Consulted)	I (Informed)	Deliverable	Date
Define technology evolution roadmap	Enterprise Architect	CIO	CFO, Business Unit Heads, Security Officer	Executive Committee	3-year roadmap	15/12

5.3. Technology KPIs Dashboard

KPI	Definition	Target	Baseline	Frequency	Owner	Data Source
Percentage of systems on supported versions	Share of systems not past vendor end-of-support	>90%	63%	Quarterly	CIO	CMDB / vendor data

5.4. Human–Cultural Risk Map (Technology Change)

Risk	Probability (H/M/L)	Impact (H/M/L)	Mitigation	Owner	Status
Resistance from business units to replacing legacy CRM	High	High	Early involvement, demos, change champions, clear	Transformation Lead	In progress

Risk	Probability (H/M/L)	Impact (H/M/L)	Mitigation	Owner	Status
			benefits communication		

5.5. 30–60–90 Day Plan for Technology Evolution

Horizon	Objective	Key Actions	Responsible	Indicators	Deliverable
30 days	Build initial technology audit scope	Identify domains, create inventory template, appoint audit owners	CIO	Scope approved, owners assigned	Audit Charter
60 days	Prioritize obsolete systems	Rate systems, estimate effort, align with budget	Enterprise Architect	Ranked list validated	Replacement Portfolio
90 days	Launch first modernization and training initiatives	Start pilot projects and learning programs	Program Manager	Initiatives started on time	Q1 Progress Report

6. Summary and Next Steps

6.1. Key messages

- **Technological evolution is a continuous discipline, not a one-off project.** Periodic audits give you a structured way to see where you stand and where you must act.
- **Obsolete systems carry visible and invisible costs.** Replacing them demands courage, planning and cross-functional collaboration, but the risks of inaction are higher.
- **New tools only create value when integrated.** A thoughtful integration strategy prevents fragmentation, improves data quality and protects security.
- **People remain at the center.** Continuous technology training ensures that your teams can adopt new tools, make better decisions and feel part of the transformation.
- **A technology radar keeps you ahead of disruption.** Monitoring trends systematically allows you to decide when to observe, test or scale emerging technologies.

6.2. Next-steps checklist

Use the table below to decide your first moves.

Next Step	Responsible	Deadline	Status (Not started / In progress / Done)	Observations
Define scope and cadence of technology audits	CIO	30/09	Not started	Use audit template from Chapter 4.1

7. Self-Assessment – Ensuring Technological Evolution

Rate each statement from 1 to 5:

1 = Strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly agree.

1. We have an up-to-date inventory of systems and integrations.
2. We run structured technology audits with clear scope and criteria.
3. Audit findings are translated into prioritized actions with owners and deadlines.
4. We have defined criteria to identify obsolete systems.
5. At least the most critical obsolete systems have approved replacement plans.
6. Replacement projects include data, process and people dimensions, not only technology.
7. New tools are evaluated based on clear business goals and integration requirements.
8. Data flows and security considerations are documented for each new tool.
9. There is a governance process to avoid proliferation of redundant tools.
10. Key role families have defined technology learning paths.
11. Technology training is continuous and connected to real projects.
12. We systematically monitor relevant technological and regulatory trends.
13. Insights from trend monitoring influence our portfolio and investment decisions.
14. There is a clear owner for technological evolution at executive level.
15. Technology evolution metrics are reviewed regularly by the leadership team.

7.1. Calculating and interpreting your score

Step 1 – Calculate

- Sum your scores for the 15 items.
- Divide by 15 to obtain an overall average between 1 and 5.

Optionally, calculate sub-averages:

- Audits and obsolescence management: questions 1–6.
- Integration and governance of tools: questions 7–9.
- Learning and trend monitoring: questions 10–13.
- Leadership and governance: questions 14–15.

Step 2 – Interpret

- **1.0–2.4 – Initial stage**
 - Technology evolution is mostly reactive.
 - Recommendation: Start with a limited-scope audit and build a basic obsolete systems portfolio. Use the 30–60–90-day plan to create momentum.
- **2.5–3.7 – Developing stage**
 - Several practices exist, but they may be fragmented.
 - Recommendation: Strengthen governance, integrate audits with budgeting and create a small technology radar function.

- **3.8–5.0 – Advanced stage**

- Technology evolution is managed strategically and reviewed at executive level.
- Recommendation: Deepen analytics, foster cross-industry learning and share your practices to attract talent and partners.

Revisit this self-assessment at least once a year to track progress.

8. Glossary (15 Terms)

1. **Technology Audit** – Structured review of systems, infrastructure, data and processes to evaluate alignment with business, risk and technical standards.
2. **Technical Debt** – Accumulated cost of shortcuts or outdated decisions in systems and architectures that make future changes harder and more expensive.
3. **Legacy System** – Older application or platform that remains in use but may be difficult to maintain, integrate or upgrade.
4. **End-of-Support (EOS)** – Point at which a vendor stops providing updates, patches or official assistance for a product.
5. **System Modernization** – Set of activities aimed at updating or rebuilding systems to meet current and future requirements.
6. **Integration Pattern** – Reusable approach to connect systems (for example, APIs, event-driven, batch processing).
7. **APIs (Application Programming Interfaces)** – Defined interfaces that allow different software components to communicate and exchange data.
8. **Technology Landscape** – Overall set of systems, platforms, tools and infrastructures that support an organization's operations and strategy.
9. **Change Management (Technology)** – Structured approach to prepare, support and help individuals and teams adopt new technologies and processes.
10. **Data Architecture** – Design of how data is collected, stored, processed and accessed across systems.
11. **Cloud Migration** – Process of moving applications, data and services from on-premise infrastructure to cloud platforms.
12. **Technology Radar** – Visualization and process used to track emerging technologies, assess their relevance and decide actions (observe, test, adopt).
13. **Digital Fluency** – Ability of leaders and employees to understand, discuss and make informed decisions about digital technologies.
14. **Cybersecurity Posture** – Overall strength of an organization's defenses against digital threats, including technology, processes and behaviors.
15. **Innovation Pilot** – Small-scale, time-bound experiment designed to test the value and feasibility of a new technology or approach.

Final Note of Gratitude

Thank you for dedicating time and focus to this material. Each concept and tool here was designed to provide clarity and strategic vision.

The fact that you are here—investing in yourself and your organization—is proof of leadership commitment.

Remember: true impact comes not only from learning but from **applying and sharing** it. May this guide support wiser decisions, deeper conversations, and more meaningful transformations.

Reference to the HBT PORTAL™

The place where each week you will find:

-  Practical ebooks.
-  Podcast summaries on Spotify.
-  Videos on YouTube.

All designed to connect innovation with the human.

 [HBT PORTAL™](#)