LAKEHILL GRC

SOLUTIONS FOR PRIVATE EQUITY INVESTORS AND THEIR PORTFOLIO COMPANIES

ABOUT LAKEHILL GRC

GRC – Governance, Risk, Compliance
- no frills, just results.

Founded in 2024 by Reto H. Wenger on a Hill overlooking a Lake. Bringing two decades of expertise, we deliver GRC solutions focused on efficiency and results. Cutting through the noise straight to the root cause: that is who we are.

«Strong Governance is only as resilient as the organizational, process and IT foundations is rests upon – without a solid structure, even the best frameworks risk collapse.»

- Reto H. Wenger

ABOUT LAKEHILL GRC

GRC: Governance, Risk, Compliance - no frills, just results.

- ICS & SOX.
- Internal Audit.
- Risk Management.
- Compliance.

About the cover image: LakeHill GRC solutions and advisory stand the test of time - shaped by deep multifaceted experience, resilient to shifting tides, and anchored in proven expertise. Just like driftwood on the shore.

OPERATIONAL VALUE CREATION THROUGHOUT THE INVESTMENT LIFECYCLE

While our core expertise lies in ICS/SOX, Internal Audit, Risk Management, and Compliance, the real value we bring extends far beyond the confines of this discipline.

Our work typically starts at the **intersection of business operations, finance, and IT - areas where inefficiencies and risks tend to concentrate.** But what we deliver is not just assurance or control, it's structural clarity. By identifying and resolving systemic weaknesses early, we help organizations not only mitigate exposure but also **unlock capacity for growth, enable more informed decision-making, and lay the groundwork for scalable, efficient processes.**

This capability is particularly valuable in Private Equity environments, where operational stability, readiness for strategic moves, and execution speed are essential. **Our approach systematically strengthens portfolio companies from the inside out - whether for accelerated growth, integration, carve-outs, or preparing for the next stage of value creation.**

LAKEHILL GRC SOLUTIONS FOR PRIVATE EQUITY INVESTORS

We are committed to:

Protect and enhance the value of your portfolio investments through robust, scalable Governance, Risk & Compliance frameworks - delivering transparency, operational resilience, and risk-based assurance across all stages of the ownership lifecycle.

The PE investor may choose to only direct, partially participate in or delegate any engagement by Lakehill GRC to the Portfolio Company's Executive Management Team.

OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

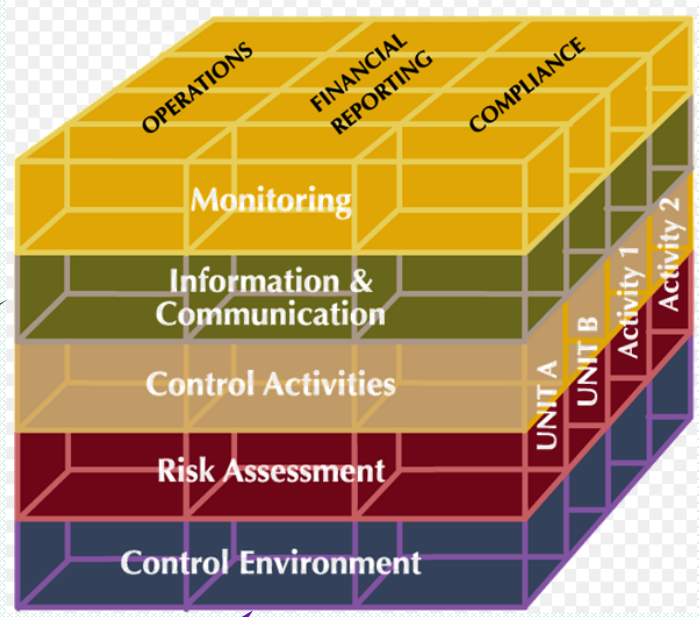
INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION:
CORE SERVICE OVERVIEW

1. Scoping – financial and IT
2. Relevant Business Process definitions & full documentation (flowcharts and narratives)
3. Significant risk definitions (for the risk-control-matrix)
4. Internal Control design drafting (Entity Level Controls, IT General Controls, Process Controls)
5. Internal Control design validation and dry-runs
6. Internal Control design remediation
7. Internal Control implementation (risk-control-matrix)
8. Internal Control performance support and evidence assessments
9. Pre-Audit assessments
10. Reshaping and restructuring IT and non-IT elements of the company's organization and process structure to get a solid foundation needed for any Internal Control framework effectiveness
11. Introducing annual internal control cycle (manuals, trainings, communication)
12. Supporting the organization in making their IT eco-system compatible for internal control requirements
13. Liasion with Internal Audit and/or External Audit (e.g. reliance agreement) for annual testing endeavors

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: COSO FRAMEWORK AS THE WIDELY ACCEPTED BEST-PRACTICE

Performance assesment over time by management

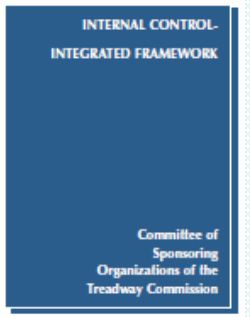
Polilcies, procedures, approvals, authorizations, verifications, etc.



Access to and identification of pertinent information

Environment and foundation enabling control to work

Identification subject to constant review: relevant for achieving our objectives



The COSO framework is recommended as the benchmark for SOX 404 reporting.

Source of Cube illustration: Sarbanes-Oxley Section 404, A Toolkit for Management and Auditors, Volume 1, PriceWaterhouseCoopers LLP, Canada, 2003

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: ELEMENTS OF ANY FRAMEWORK

The three framework foundational elements

Financial Scoping (Balance Sheet and Income Statemt)

Account example:
Accounts payable

Business Processes influencing the scoped accounts

Process example:
Sourcing

Determine risk in those Business Processes

Risk example:
Payments posted in absende of 3-way-match

The three framework internal control categories

Entity level controls

Control example:
Entity Level Control on supplier due diligence

Business Process Controls

Control example:
System matches PO, delivery note, invoice

IT General Controls

Control example:
ERP access is restricted to authorized staff

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: PROCESS DOCUMENTATION STEPS

Step #	Activity	Input	Output	Roles
1	Review process list and check availability of already existing documentations	Available documents (check validity)	Full process inventory to be documented	Program owner
2	Breakdown processes (1) defined above	Program relevant list of processes	Breakdown of processes	Shared: Program owner and BPOs
3	Document the processes	Desk research, interview notes	Draft process documentation	Shared: Program owner and BPOs
4	Review, ensure processes connect end-to-end, eliminate redundancies	Draft process documentation	Reviewed documentation	Program owner
5	Obtain approval	Reviewed documentation	Approved documentation	CFO (seek Auditor endorsement)

(1) – see next slide on Process Breakdown

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: PROCESS BREAKDOWN - EXAMPLE

Layer	Label	Target description
1	Process	One level below the significant process (see also scoping result, e.g. sourcing), lies the «Fixed Asset physical observation» which is the layer #1 Process in this example
2	Capability	A functional capability that contributes to the above, e.g. planning xyz
3	Activity	A subset of actions needed to complete the activity, e.g. ordering xyz
4	Task	Task as part of the process inherent actions, e.g. submit the order form
5	Action	Granular duty, e.g. filling each field of the order form

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: CONTROL DOCUMENTATION STEPS

Step #	Activity	Input	Output	Roles
1	Review (already existing, if any) control narratives	Available control documentation (if any)	Applicable and validated starting point, identified control owners	Program owner
2	Customize (if need be) control narratives	= Output previous step	Valid control narratives	Nominated control owner(s)
3	Review drafts establihsed	= Output previous step	Validated control narratives	Business Process Owner(s)
4	Review controls (from a control effectiveness perspective)	= Output previous step	Reviewed control documentation	Program owner
5	Sign-off control	= Output previous step	Approved controls read for operational performance	CFO
Ongoing	Annual sustainability: Perform, monitor, remediate	Evidence	Annual updates to scoping and controls	Program owner

Guiding principles: What the paper says has to agree to how the process works and – from an Auditor's perspective - what's not documented is not done (-> control performance consistency is key)

INTERNAL CONTROL SYSTEM (ICS & SOX) IMPLEMENTATION: IT GENERAL CONTROLS – EXAMPLE STARTING POINT

ITGC control category	Financially relevant ERP	Consolidation software	Production software	Sales software	Other (in-house apps, end-user controls)
Access	SOC report available, need to complement (see end of SOC report)	Assurance from provider (no SOC, to be examined in detail)	In-house developed – need to shape everything from scratch	To be evaluated with in-house ticketing tool	Confirm each application's financial relevance, subsequently (if need be) assess controls therein as a first step
Change				Tentatively out-of-scope as SaaS, need to confirm details with vendor	
Continuity		Other provider			
Security		unknown			

Strong recommendation: every application has an owner (one designated competent individual) within the organization who bears the sole IT general control implementation resopnsibility.

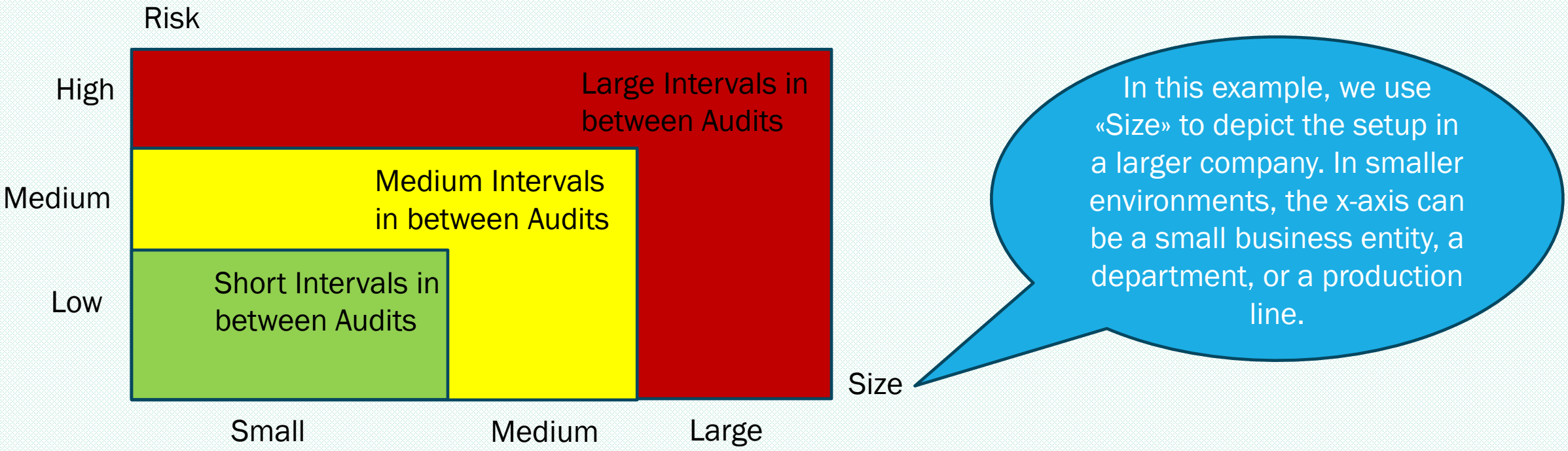
OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

INTERNAL AUDIT – PLANNING & ENGAGEMENTS:
CORE SERVICE OVERVIEW

1. Shaping the Internal Audit function (following IIA Standards)
2. Creating the IA risk based planning – process and deliverables
3. Establishing the annual IA engagement schedule – including resource management
4. Implemeting the IA manual – covering the entire activity and its deliverables (following IIA Standards)
5. Supporting the first annual risk-based planning cycles with the auditees and Mangement/Board/AC
6. Designing the company Internal Audit Report (to be used for each engagement)
7. Orchestrating the quarterly high risk (or exception) reporting to Management/Board/AC
8. Implementing IA high value add features – see following slides
9. On-the-job training of IA management and IA staff from engagement planning to final report issuance
10. Aligning IA activities with other assurance functions
    (Internal Control, Compliance, Legal, Investigations)
11. Ensuring IA continuity over the years so that entire scope (e.g. Audit Universe) gets covered
12. Strengthening unbiased, organizationally independant and professional conduct at all times
13. Supporting IA in consultancy engagements for select projects (outside of the Audit Engagements)

INTERNAL AUDIT:
ANNUAL RISK-BASED PLANNING RATIONALE



INTERNAL AUDIT:
ANNUAL RISK-BASED PLANNING – FIND THE AREA AT RISK - EXAMPLE

Likelihood

Sources to review:
- Risk Management
- Prior Audit Reports, if any
- External Sources (consider environmental variables)

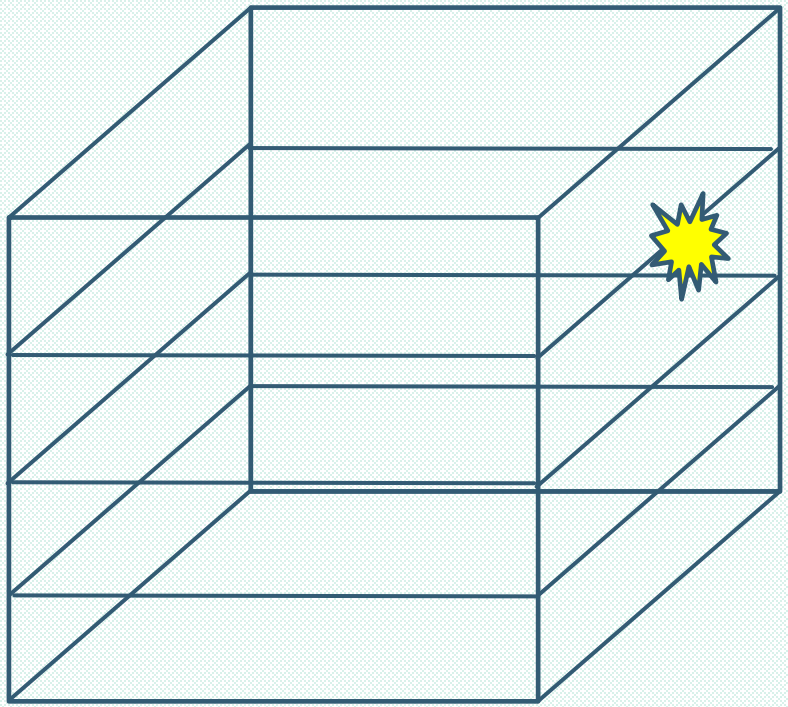
Impact

Sources to review:
- Risk Management
- KPIs (fin and non-fin)
- Past irregularities

3rd dimension (if needed)

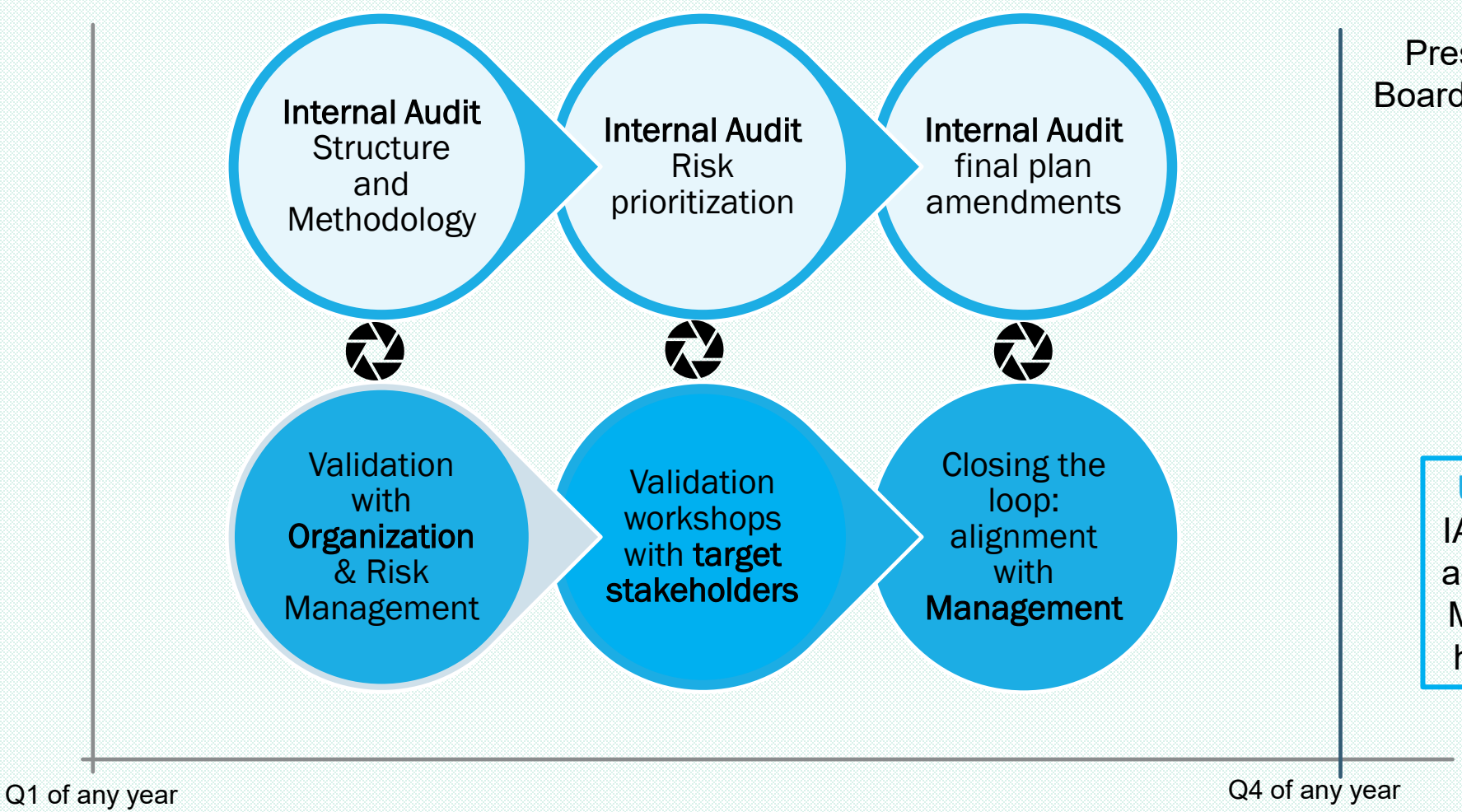
Possible considerations:
- Size of area considerations
- Segment/Product controlling
- Business Model
- Organizational dependencies

Example: Fixed Asset Valuation



Source of Cube illustration: Sarbanes-Oxley Section 404, A Toolkit for Management and Auditors, Volume 1, PriceWaterhouseCoopers LLP, Canada, 2003

INTERNAL AUDIT:
ONE ITERATIVE APPROACH TO BUILD THE ANNUAL IA PLAN



Presentation of Plan to Board and/or Management

Underlying rationale: Annual IA planning is most impactful if it addresses risk identified by Risk Management. That will produce high value audit engagements.

INTERNAL AUDIT DELIVERING REAL VALUE: «NO IDENTICAL REPEAT FINDINGS» - PLANNING ELEMENT

"Severe" Audit Observation found anywhere in the company

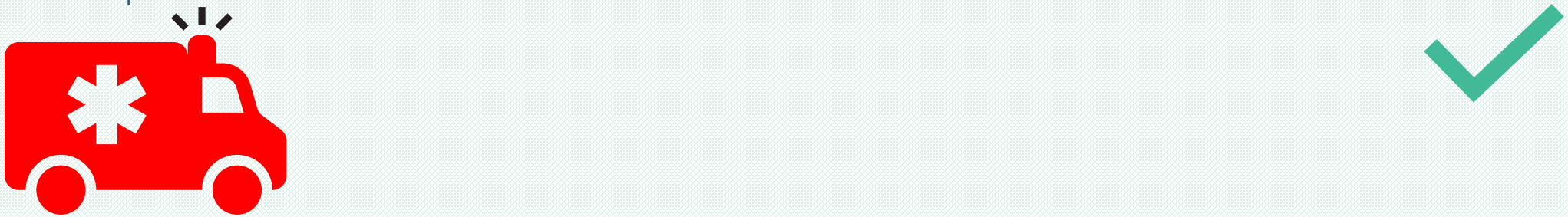
→

Observation is reported and process/control **remediation is immediately initiated to avoid reoccurrence of this same finding**

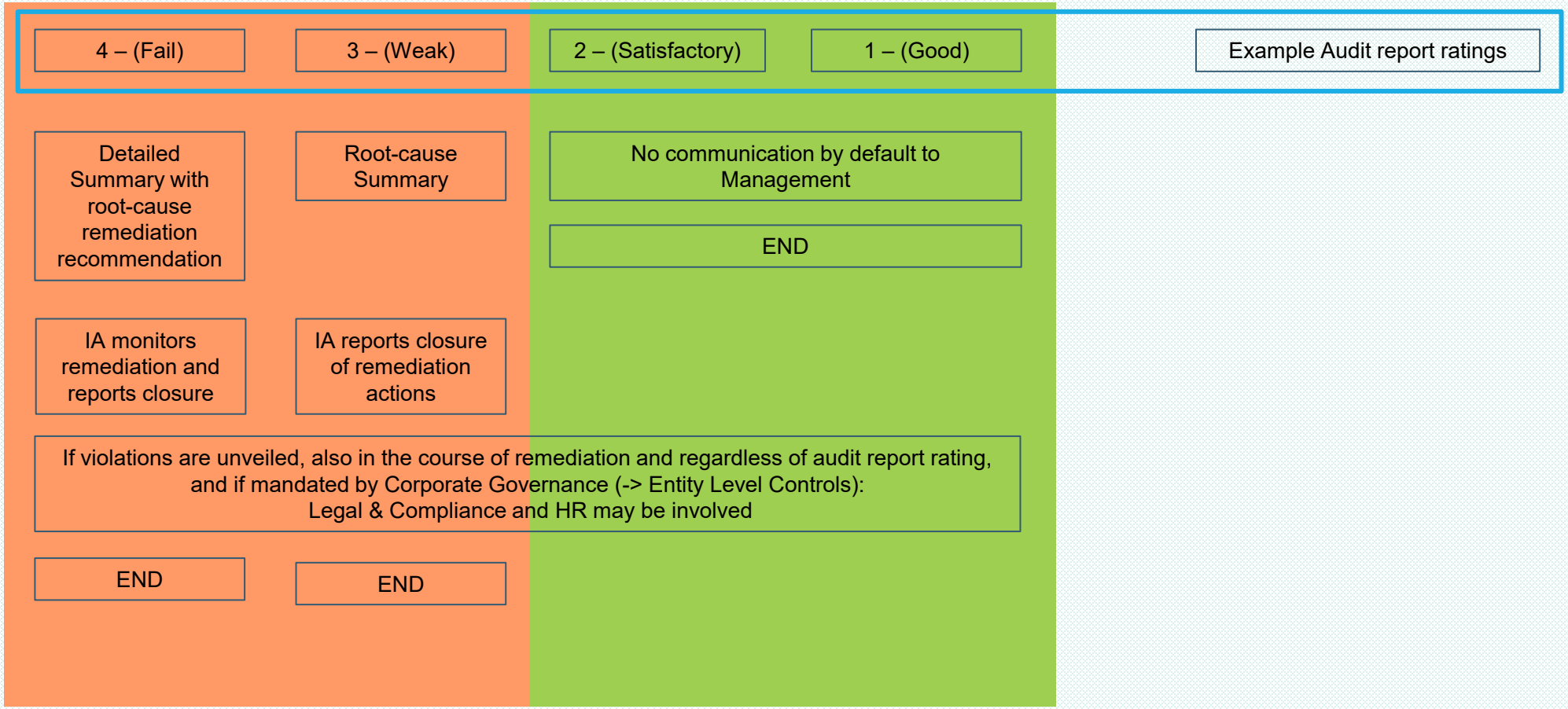
→

The process underlying the finding is **remediated company-wide**

↓



INTERNAL AUDIT DELIVERING REAL VALUE: CONSEQUENCE MANAGEMENT FOR MAJOR OBSERVATIONS



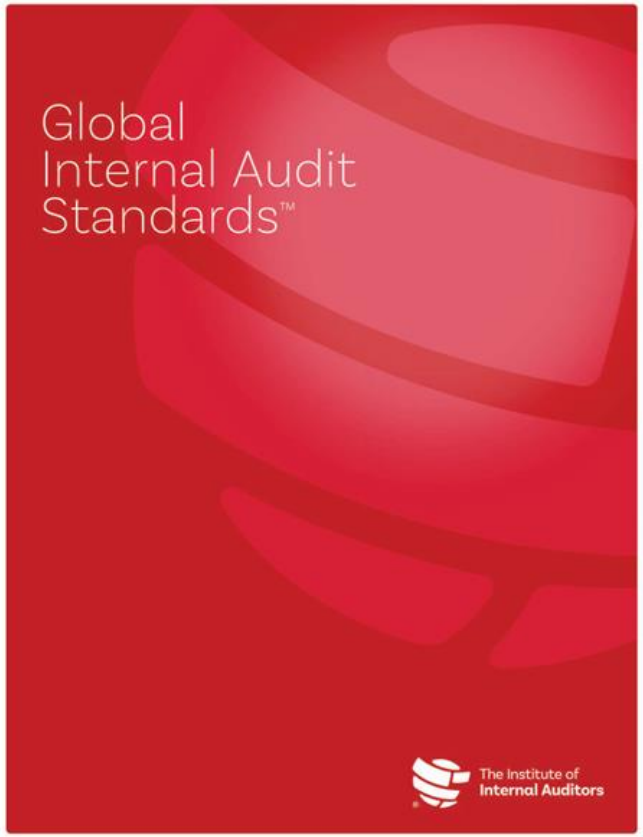
OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

INTERNAL AUDIT – PLANNING & ENGAGEMENTS:
CORE SERVICE OVERVIEW

1. Shaping the Internal Audit function (following IIA Standards)
2. Creating the IA risk based planning – process and deliverables
3. Establishing the annual IA engagement schedule – including resource management
4. Implemeting the IA manual – covering the entire activity and its deliverables (following IIA Standards)
5. Supporting the first annual risk-based planning cycles with the auditees and Mangement/Board/AC
6. Designing the company Internal Audit Report (to be used for each engagement)
7. Orchestrating the quarterly high risk (or exception) reporting to Management/Board/AC
8. Implementing IA high value add features – see following slides
9. On-the-job training of IA management and IA staff from engagement planning to final report issuance
10. Aligning IA activities with other assurance functions
    (Internal Control, Compliance, Legal, Investigations)
11. Ensuring IA continuity over the years so that entire scope (e.g. Audit Universe) gets covered
12. Strengthening unbiased, organizationally independant and professional conduct at all times
13. Supporting IA in consultancy engagements for select projects (outside of the Audit Engagements)

INTERNAL AUDIT ENGAGEMENTS: STRUCTRUE AND DISCIPLINE – GLOBAL IA STANDARDS (*)



Guiding principle: All our Internal Audit support engagements are conducted in accordance with the Global Internal Audit Standards promulgated by The Institute of Internal Auditors, specifically:

Principle 13 – Plan Engagements Effectively
Principle 14 – Conduct Engagement Work
Principle 15 – Communicate Engagement Results and Monitor Action Plans

As we are an external provider, adherence to these Standards is inherently limited

(*) see also: https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/free-documents/complete-global-internal-audit-standards/ accessed on July 2nd, 2025 1100h AM CET

OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

RISK MANAGEMENT:
CORE SERVICE OVERVIEW

1. Define purpose and scope (ERM, operational, finance, cyber, projects, etc.)
2. Secure sponsorship and resources (top level buy in – no bottom up initiatives tend to sustain)
3. Engage in supporting the appointment of a Risk Officer
4. Develop a Risk Management Framework
5. Build Foundational Tools and Policies
6. Identify and Assess Risks
7. Define Mitigation Actions and Owners
8. Establish Risk Governance and Reporting
9. Train and Communicate
10. Integrate with other Functions (ICS, IA, Compliance, Investigations, Legal)
11. Monitor, improve and further develop

RISK MANAGEMENT:
EXAMPLE FOUNDATION AND STRUCTURING

Macro Environment	Legal & Regulations	Financial
Politics	Litigations	Liquidity
Economy	Fraud & Corruption	Controlling
Disaster	Compliance	Taxation
		Insurance
		Credit Default

Business Support/Plan	HR	Corporate Value
Organization	Talent (sourcing, development, retention)	Reputation
Procurement	Know-how	Communication
Projects	Employer branding	Corporate Brand
Business Portfolio	Succession (next leadership generation and functional experts)	Investor Relations
		Industry presence

RISK MANAGEMENT:
EXAMPLE DEFINITIONS TO BE FURTHER REFINED

Macro Environment	Politics	The risk that political instability, changes of the government or increased political pressure from the public or NGOs which leads to a crisis/conflict. The opportunity that political stability supports economy and investment programs
	Economy	The risk that the economics development in a country will significantly have an influence on our market presence
	Disaster	The risk that a major disaster (nature- or man made) will impact the operations or assets of the company
Legal & Regulations	Litigations	The risk that existing or future litigations will have an impact on our business
	Fraud & Corruption	The risk that the company falls victim to fraud and corruption
	Compliance	The risk that the company is not in adherence to existing laws and regulations which might result in civil or criminal proceedings, financial consequences and in loss of reputation
	ICS/SOX	The risk that the company does not meet ICS/SOX requirements
Financial	Liquidity	The risk that the company will not generate sufficient cash flow or will not have access to funding or that there will be an adverse impact by FX or interest rate changes
	Controlling	The risk that management cannot effectively measure and monitor the company, including the risk of unreliable budgets, forecasats and financial reports
	Taxation	The risk that the company does not comply with applicalbe tax regulations or does not strategize to optimize tax expenses
	Insurance	The risk that the company's insurance program will not adequately cover the financial impact for potential detrimental events
	Credit Default	The risk that customers default on payment resulting in significant write-off and collection costs
Business Support/Plan	Organization	The risk that the general organiaztion of the company does not support the business effectively
	Procurement	The risk that procurement is not done in the most effective way so that poential benefits will not be realized
	Projects	The risk that projects cannot be delivered to the customer
	Business Portfolio	The risk that different business activities are not providing the right mix for a sustainable business model which meets stakeholder and/or shareholder expectations
HR	Talent	The risk that the company does not attract, develop and retain the right people in the right places to reach its targets
	Know-how	The risk that knowledge is not retained in the organization with own staff
	Employer branding	The risk that the company brand as an employer is not well perceived in the market
	Succession	The risk that succession management is not done effectively
Corporate Value	Reputation	The risk of loss of the company's reputation (internal or external) which may result in mistrust against the company
	Communication	The risk that internal or external communication will not have the desired effects
	Corporate Brand	The risk that the coporate brand value is not well perceived in the market
	Industry presence	The risk that the professional contributions to the industry community are not well perceived

OUR GRC SOLUTIONS: HIGH-LEVEL OVERVIEW

1. Internal Control System Implementation (ICS & SOX)
2. Internal Audit - Planning
3. Internal Audit - Engagements
4. Risk Management
5. Compliance

COMPLIANCE:
NON-REGULATED CORE IMPLEMENTATION SERVICES

- Design and roll-out of company-specific Compliance Frameworks aligned with values and risk profiles
- Development and implementation of practical policies, procedures and internal standards that embed compliance matters into daily operations (-> no additional bureaucracy silos)
- Setup of Compliance Tools and Processes for consistent documentation, reporting and issue tracking (e.g. Whistleblower systems)
- Establishment of monitoring routines and consequence management for policy violations
- Support of annual cycles, including content updates, ownership tracking and training/communication
- Close collaboration with your in-house or external legal counsel to ensure legally sound yet oprationally viable implementation
- Strong focus in anything we do on business-oriented and scalable compliance – no unnecessary complexity
- Empowerment of internal teams through awareness sessions, face-to-face trainings and coaching – no check-box only exercise

THANK YOU FOR YOUR ATTENTION

About LakeHill GRC:

- LakeHill GRC operates independently under Swiss and U.S. legal frameworks**.** LakeHill GRC is a sole proprietorship based in Wilen bei Wollerau, Switzerland, and also registered as an LLC in the State of Florida, USA. These are two legally distinct entities that do not share client data, operations, or contractual obligations. The only commonality is a shared public-facing website, used solely for informative and promotional purposes. Swiss-based clients are exclusively served by the Swiss entity, subject solely to Swiss law and jurisdiction.
- The founder and owner, Reto H. Wenger, is overseeing and providing all core services, with access to a wide network of seasoned professionals, within regulated and non-regulated services, both in the central Switzerland region, the DACH region and globally.
- LakeHill GRC does not engage in any activities that full under regulated professional services. This includes, but is not limited to, statutory financial audits, legal representation or advice, tax advisory services requiring formal authorization or any other services subject to regulatory licensing or oversight under US, Swiss or EU law. Furthermore, LakeHill GRC does not provide any services that involve or require compliance with the Swiss Anti-Money Laundering Act (AMLA), the Financial Institutions Act (FinIA), or the Financial Services Act (FinSA).

LakeHill GRC

Reto H Wenger, Founder and Managing Director
BSc. | CAS | EMBA | Certified Internal Auditor

In the United States:
LakeHill GRC LLC, 7901 4th St. N Ste 300, St. Petersburg, FL, 333702, info@lakehillgrc.com, +1 407 456 7353, lakehillgrc.com
In Switzerland:
LakeHill GRC Reto H. Wenger, Hungerstr. 51, 8832 Wilen b. Wollerau, reto.h.wenger@lakehillgrc.com, +41 79 613 4990, lakehillgrc.com/de