LAKEHILL GRC

WHITEPAPER: GRC READINESS FOR HIGH-GROWTH SCALE-UPS

DIRECTIONAL GUIDANCE FOR FOUNDERS, OWNERS, MANAGERS, BOARD MEMBERS AND INVESTORS

TARGET AUDIENCE AND PURPOSE OF THIS DOCUMENT

AUDIENCE - this document is intended for:

- **Founders, Board and Management members** of high-growth scale-ups.
- **Prospective and existing investors** of any type engaging with high-growth scale-ups.
- **Law firms, specialized financing advisory boutiques and other professional** intermediaries involved in structuring, advising on, or executing financing transactions for high-growth scale-ups.

PURPOSE - this document is intended to:

- Provide **education and initial guidance** for high-growth scale-ups on Governance, Risk, Compliance and any underlying structural/process/system requirement in order to make it work.
- To **familiarize and raise awareness** of what the preparation for a successful Financing Round, Private Equity Investment, Family Office Investment, Venture Capital, Corporate Investor, Angel Investor or Loan financing will entail.
- To **inform that modern GRC at large is largely system integrated** without the exhaustive need for manual processes and resource intense bureaucracy.
- To **increase confidence** that through timely planning and a disciplined plan execution, a vast majority or GRC implementation deliverables can be achieved from within the organization.

ABOUT LAKEHILL GRC

GRC – Governance, Risk, Compliance. And much more to make it work - 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

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

GRC AND ITS BUILDING BLOCKS IN A NUTSHELL

Governance	Are we directed and controlled properly? Decisions, accountabilities, oversight, standards, BoD & Management responsibilities, etc.
Risk	What could prevent the company from achieving its objectives? Risk identification & assessment, mitigations, monitoring, reporting, etc.
Compliance	Are we meeting all applicable laws, standards and committments? Regulatory obligations, industry standards, financial reporting, policies, commitments, etc.

An effective GRC framework strengthens the company's ability to **operate as a going concern**:

- It is THE paramount element for **investors to decide favorably** (investment, valuation, exit, IPO, etc.).
- It ensures clear ownership, strategic unambiguity and transparency **vis-à-vis all stakeholders.**
- It covers risks that may have a financially **detrimental impact** on the company.
- It provides **assurance** on regulatory adherence, documentation accuracy and evidence and audit readiness.

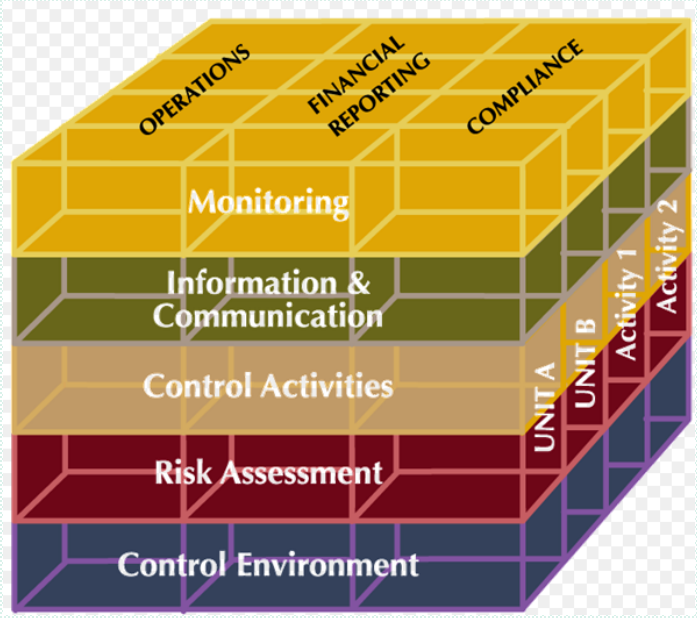
Suffering a detrimental event that was preventable – including going out of business – is not ever an option.

GRC AND ITS BUILDING BLOCKS IN A NUTSHELL

Deriving select practical building blocks of GRC from COSO

- Control Environment:
  Tone at the top, Code of Conduct, Policies.
- Internal Controls:
  Preventive and detective controls (system-embedded).
- Risk Framework;
  Risk register, assessments, monitoring cadence.
- Policies and Procedures:
  Documented standards and SOPs.
- Reporting & Transparency:
  BoD reporting, KPIs, KRIs.
- Accountability & Ownership:
  Defined risk and control owners.
- Audit & Assurance:
  Internal and External Audit – independent assurance.

COSO as the widely accepted best-practice benchmark



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

Modern GRC is (ERP-)system and process integrated: no spreadsheets and box-ticking bureaucracy.

GRC AND ITS BUILDING BLOCKS IN A NUTSHELL

High-level sequence of activities: from greenfield to first operational cycle

1. Scoping

- Determine the law, requirement or standard you are subject to.
- Apply the scoping approach (see following slides).
- Plan (with your own involvement) and budget
- Secure resources.
- Involve all stakeholders and layers of the organization.

2. Risks and Controls

- Consider risk management re-purposing you already have .
- Use existing, update or draft process documentation.
- Identify and assess the risks (material: tied to financial reporting – significant: tied to complexity and impact- DMRM).
- Draft controls that mitigate those risks (1:1 and 1:n).

3. Operate and Test

- Deploy the controls.
- Ask owners to self assess and propose corrective measures.
- Sustain the controls framework (12 months) – no changes. allowed by default.
- Test the controls (preferably by an independent party).
- Subject the controls to external scrutiny (as may be the case).

Plan wisely: third parties can do most of the documentation, you will have to own the performance.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

WHY AND WHEN GRC ASSUMES IMPORTANCE (AND URGENCY)

Financing event	Regulatory scrutiny	Reporting obligations	Litigations
No investor, big or small, domestic or foreign (Financing Round parties, Private Equity, Debt Financing, Family Office, Bank) **will even consider investing in a structure lacking controls to secure the investment** (oftentimes prevented by their statutes). **Going concern at risk!**	Violations (intentional and non-intentional) of prevailing laws, regulations and standards (such as e.g. MDR, GDPR, CSRD) **may have severe consequences** ranging from being banned from markets, having permits revoked to penalties & legal fees. **Going concern at risk!**	Non-adherence to reporting obligations **equals the incapacity to produce reliable information** (financial, non-financial) which may trigger erosion of trust at large all the way to the regulator taking action (sanctions, delisting, market abuse, proceedings) **Going concern at risk!**	At any given time in the course of business, a party may take legal action against the company alleging a wide series of damages which, depending on the jurisdiction(s) one operates in, **may bear the risk of public reprimand & high cost** to eventually settle. **Going concern at risk!**

In any of those scenarios, effective GRC substantiates serious business conduct –it pays for itself.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

FRAMING THE NEXT FOUR CHAPTERS: CONTEXT REQUIREMENT

On the following slides covering:

1. The scoping exercise – how to scratch from start,
2. Entity Level Controls (ELC),
3. IT General Controls (ITGC) & AI Governance and
4. Business Process Controls (BPC) & AI Enhancements,

a set of randomly chosen examples, illustrative and non-exhaustive, intended to provide an overview of the breadth of potential requirements, are shown.

Only a subset may be relevant for any individual organization.

Example only

THE SCOPING EXERCISE – HOW TO START FROM SCRATCH

The non-exhaustive universe of GRC requirements calling for IT/process and control implementation:

Financial Reporting & Internal Control Regulation
ICS, SOX (US, JP, CA), German Corporate Governance Code, French Financial Security Law, EU Statutory Audit Directive
IT Governance & Cybersecurity Frameworks
ISO 27001, NIST, COBIT, ITIL, SOC 2
Data Protection & Privacy Regulations
GDPR, Swiss Federal Act on Data Protection, California Consumer Privacy Act
Risk Management & Governance Standards
COSO ERM Framework, ISO 31000 (Risk Mgmt), IS 37301 (Compliance Mgmt), ISO 37001 (Anti-Bribery)
Operational Assurance & Outsourcing
ISAE 3402, SSAE 18, SOC 1, SOC 2, SOC 3
Industry-specific Compliance
EU MDR, FDA 21 CFR Part 11 and 820, ISO 13485, AMLA, Payment Card Industry Data Security Standard
ESG & Sustainability Governance
CSRD, ESG, Task Force on Climate-related Financial Disclosures, Global Reporting Initiative
AI Governance
EU AI Act, NIST AI Risk Management Framework, ISO 42001 (AI management system)

Example only

THE SCOPING EXERCISE – HOW TO START FROM SCRATCH

Financial scope	To **determine what really matters for financial statement reliability** and where a company needs to set its focus (with a 95% threshold for example).
Entity Level scope	To understand **which parts of the company**, its business units or manufacturing sites **are in scope**, typically based on KPIs such as revenue, total assets, profit contribution.
Process Level scope	To **analyze which business processes affect** the overall scope; some are standard and others vary depending on the nature of the business.
Information Technology scope	To define which **IT elements** are involved **in the value creation** at large.

Now – and only now – a risk and control discussion renders any tangible benefit.

Example only

THE SCOPING EXERCISE – HOW TO START FROM SCRATCH

ISAE 3402 scoping	To define services regarding your client's financial reporting hence the scoping is **geared towards client expectations.**
ESG scoping	To define **what sustainability topics truly matter** for the business and its stakeholders and what topics are material.
CSRD scoping	To define **a series of technical considerations** with required coverage of upstream value chain, downstream value chain as to a set of specific KPIs.
MDR scoping	To understand **what conformity and compliance obligations to follows.** It defines how and to what extent your medical products/organization fall under the EU MDR (FD&C Act for the US).

There is no one-size-fits all scoping recipe other than the foundations for any framework needing to be solid.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

Example only

ENTITY LEVEL CONTROLS (ELC)

Categories

1. Overall Company Analysis.
2. BoD & Committee(s) Charters.
3. Risk Management.
4. Internal and External Audit.
5. Compensation.
6. Tone at the Top.
7. Code of Conduct.
8. Whistleblower Programs.
9. Acceptable Business Practices.
10. Anti-Fraud and Anti-Corruption.
11. Organizational structure.
12. Officers' profiles.
13. Technology Governance.
14. Business Ethics.
15. Staff communication.
16. External relations.

Narratives

Entity Level Control narratives typically **do not address a specific** risk, system or transaction.

They operate at a higher level to have a **pervasive impact** across the organization.

They are **the foundation** (and thus to some extent also the fallback control) to the internal control framework.

Verbiage encapsulates **governance ownership at large** by BoD, BoD committee and C-Suite. Most of it is publicly disclosed as it build trust with customers, shareholders, authorities.

Risk Mitigation

Unlike business process controls addressing a concrete risk, Entity Level Controls are worded to **address COSO principles,** such as:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring Activities

COSO guidance lists close to 90 points of focus (rather than detective and/or preventive process risk mitigation).

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

Example only

IT GENERAL CONTROLS (ITGC) & AI GOVERNANCE

Categories	Narratives	Risk Mitigation
1. **Access** • Access granting, modifying and revoking. • Rights and Roles. • Logical access. • Physical access. 2. **Change Management & Change** • Mitigating the unintended impact any change inherently bears. 3. **Business Continuity & Availability** • Ensuring IT services availability in man- or nature made disaster scenarios. 4. **Security** • Protection: confidentiality, integrity, availability objectives.	Ideally, a company operates an IT eco-system with Applications **that already contains a high level of assurance,** best evidenced by a System and Organization Controls (SOC) Type 2 report upon which it can build its own controls (also referred to as user entity responsibilities). In absence of the above, the implementation of **ITGCs calls for various professionals** to implement, perform, monitor and maintain. ITGC narratives (and underlying processes) are of **technical language** addressing all system inherent risks as per the four categories.	Example risk mitigation include: 1. Access **Unauthorized access** to and usage/disclosure of data and modification thereto. 2. Change **Erroneous/unapproved batch** upload to a core module of the production system. 3. Continuity **Incapacity to restore** DSO and thus to collect outstanding balances. 4. Security **Firewall configurations** are not reviewed, approved and documented.

Example only

IT GENERAL CONTROLS (ITGC) & AI GOVERNANCE

AI Governance

Different frameworks in place with broadly consistent pillars:

- **Accountability & Oversight**
  -> Ownership & Governance for AI.
- **Risk & Impact Management**
  -> Bias, ethics, fairness.
- **Transparency & Explainability**
  -> Logic, lineage and traceability.
- **Data Governance & Quality**
  -> Integrity, bias mitigation.
- **Security & Robustness**
  -> Protection, adversarial testing.
- **Change & Lifecycle Management**
  -> Control, model drift monitoring.
- **Human Oversight**
  -> Human control to override.

AI Governance: mapping attempt to the 4 COBIT categories

Access:
Who can train a model, modify a prompt, deploy a model and access model training data?

Change Management & Change
Who can retrain a model, update its algorithms, introduce prompt modifications and refresh data sets?

Business Continuity & Availability
How are we protected in case of continuity when AI outputs are unavailable, what are the fallback mechanisms when the AI model fails, how can we manually override to AI model?

Security
Are we on the safe side with regards to AI model theft, adversarial attacks, data poisoning, API abuse?

AI Governance extends to address ethical risks, model behavior, transparency and lifecycle accountability.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

Example only

BUSINESS PROCESS CONTROLS (BPC)

Categories

1. **Book-to-Report**
   - Closing process.
2. **Order-to-Cash**
   - Master Data (client).
   - Pricing & Order Entry.
   - Distribution & Logistics.
   - Invoicing & Collection.
3. **Purchase-to-Pay (OPEX & CAPEX)**
   - Master Data (vendor).
   - Purchases (PR to PO).
   - Receipt & 3-way-match.
   - Inventory and Assets.
   - Payment & Cash.
4. **Hire-to-Retire**
   - Payroll.
5. **Production**
   - Maintenance.
   - Consumables.
   - Scheduling.

Narratives

Controls are worded **very specifically** to either prevent or detect the risk (which translates into the control objective).

Controls can be **manual, IT-dependent or automated**/system embedded.

They state the control activity, what is needed to perform the control, what the outcome is **and how exceptions are handled.**

Exceptions handling is the detection of the event, the investigation triggered, the resolution achieved and the closing of case with supporting evidence.

Risk Mitigation

Risks (control objectives) may include:

- Posting to wrong period.
- Inaccurate Fx rate applied.
- Inaccurate accruals booked.
- Stock balances are wrong.
- Provisions not recorded.
- Unapproved discounts applied.
- Shipments not recorded correctly.
- Purchaser approves order and directs receipt of goods.
- Duplicate orders / duplicate payments.
- Critical vendor defaults.
- Overtime is self-approved and paid out.
- Former employee bank account changed to other beneficiary.
- Preventive maintenance not scheduled leading to disruption.

Example only

BUSINESS PROCESS CONTROLS (BPC)

Traditional manual control	AI Enhancement
Manual Journal entry controls: • Manual review of unusual entries. • Focus on large items. • Period-end sampling. • Time consuming investigation. • Resolution, documentation. • Evidence production (PBC).	**AI Efficiency gain:** • Automated risk scoring for every journal entry. • Identification of high-risk combinations (e.g. posting user, posting time, accounts posted to and posting text). **AI Assurance gain:** • Detection of round-number bias, end-of-period management override, Segregation of Duties circumvention, Behavioral deviation from posting user history.
3-Way Match (PO-GR-IR) • Invoices matches PO and goods receipt (in ERP). • Exceptions flagged to user. • Follow-up actions remain manual. • Entirely manual for Services.	**AI Efficiency gain:** • Smart tolerance thresholds (historically based) with automatic resolution of recurring legitimate deviations and vendor behavior learning. **AI Assurance gain:** • Detection of vendor collusion patterns, identification of invoice splitting, detection of abnormal price development, recognition of procurement bypass behavior.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

SELF ASSESSMENT AND AUDITING

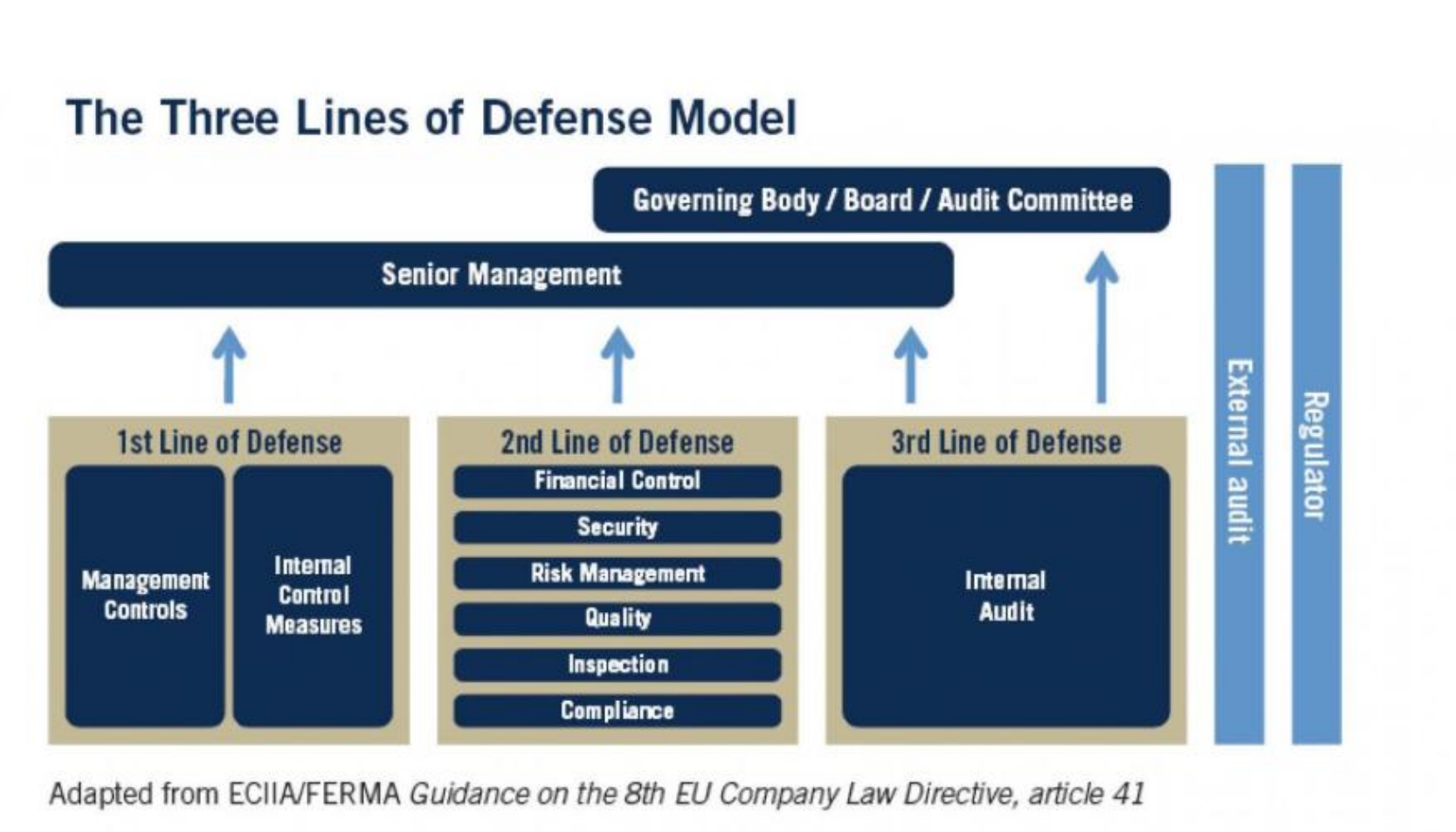


Illustration accessed at https://internal-audit-strategy.com/3lod-neu-aufage on March 3rd, 2026

When planning and executing with discipline, a company can do 80% from within.

Self-Assessment

To be orchestrated by the organization's LoD 1 and LoD2 with ample time to remediate errors.

Internal Audit

Planned with agreed upon scope, reporting to the BoD/AC with findings to be addressed timely.

External Audit

Failure is not an option anymore. Results will be reported to the BoD/AC or even AGM/EGM or Public.

HIGH-GROWTH SCALE-UPS GRC SOLUTIONS

1. GRC and its building blocks in a nutshell
2. Why and when GRC assumes importance (and urgency)
3. The scoping exercise – how to start from scratch
4. Entity Level Controls (ELC)
5. IT General Controls (ITGC) & AI Governance
6. Business Process Controls (BPC) & AI Enhancement
7. Self Assessment and Auditing
8. Q&A

Q&A

Your questions?

Your four key take-aways!

1. **Fry the big fish,** unless subjected to a regulatory framework, let go of the small insignificant and immaterial topics – they won't move the needle ever.
2. **Work smarter, not harder.** Understand the risk, its root cause, the systems and dependencies and then put the control in place: in a system, as part of a routine, in everyone's job description. Don't compare two spreadsheets by creating a third one – that is not reliable assurance.
3. **No Governance with AI and/or automation without knowing what's underneath.** Multiplying an error and thus making it uncontrollable is not what you need.
4. **Start whilst you are still in control.** When others start asking questions – especially when in context of the financing you need – it is usually too late.

Effective GRC is fit-for-purpose, conducive to your size and nature of business, and always pays for itself.

APPENDIX: OUTLOOK – THE ADMINISTRATIVE ROLE OF TOMORROW

	Today (traditional)	Tomorrow (AI-enabled)
Tasks	1. Executes transactions. 2. Performs reconciliations. 3. Follows fixed check-lists and rules. 4. Works periodically. 5. Performs controls manually.	1. Supervises automated processes. 2. Reviews AI-flagged exceptions. 3. Interprets AI risk scoring. 4. Engages in real-time monitoring. 5. Oversees and validates controls.
Skills	1. Good Excel and Power BI skills. 2. Strong org and time management. 3. Excellent communication skills. 4. Prior administrative experience. 5. High school & business college.	1. Literate in interpretation of AI model. 2. Managing workflows and exceptions. 3. Interpret and explain AI outputs. 4. Experience with automation. 5. Ability to adapt to digital tools.

Many roles shift from task execution toward exception handling, interpretation and supervision. This applies to administrative elements in all roles, e.g. Accounting, Auditing Banking, Fiduciary, HR, Procurement, Logistics, Hospitality, Medical, Legal, Healthcare, Pharmaceutical, Real Estate etc.

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).

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

LakeHill GRC LLC, 7901 4th St. N Ste 300, St. Petersburg, FL, 333702, USA
info@lakehillgrc.com, Phone: +1 407 456 7353

LakeHill GRC, Hungerstrasse 51, 8832 Wilen bei Wollerau, Switzerland
reto.h.wenger@lakehillgrc.com, Phone +41 79 613 4990

https://www.lakehillgrc.com