LAKEHILL GRC

WHITEPAPER: TRANSITIONING THE INTERNAL CONTROL FRAMEWORK FROM SOX (US) TO ICS (SWITZERLAND)

ABOUT LAKEHILL GRC

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

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

ABOUT LAKEHILL GRC

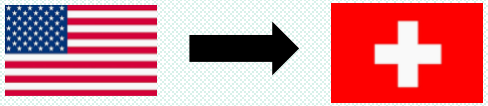
GRC – Governance, Risk, Compliance
- no frills, just results.

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

Introduction: ICS effectiveness post de-listing



US SOX environment

- 200+ (key) controls
- ICFR focus (accuracy/timeliness)
- US (SEC) regulations
- Impact (risk) on listing & share price
- Documentation expectation
- Governance & Accountability
- Anti-Fraud Objective
- Strong ITGCs

Challenge: shrink without shrinkage

Swiss ICS environment

- Lower number of (key) controls
- ICFR focus remains
- Regulatory similarities, less rigid
- Board Responsibility

SOX to ICS-oriented: less controls does not automatically translate to a lower assurance level

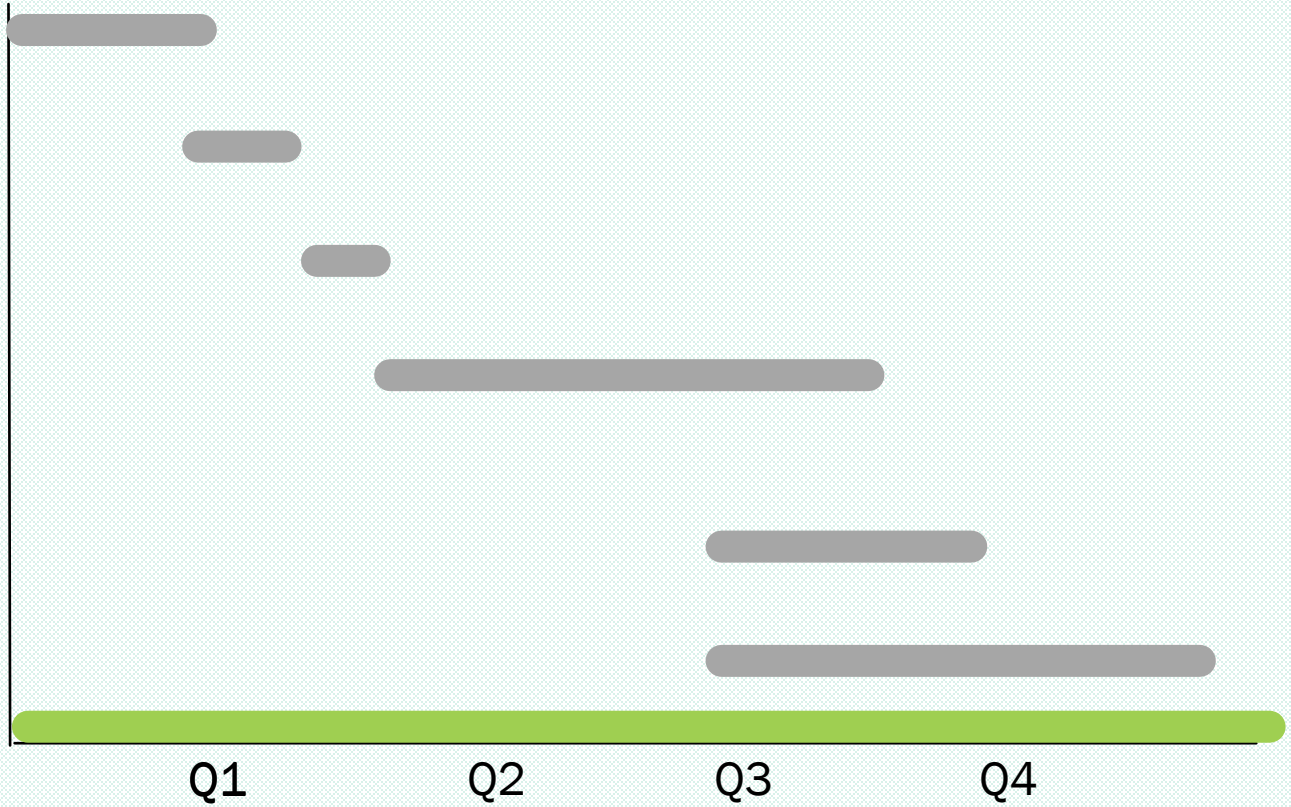
Context & Challenges: effectiveness and simplification (*not vs.!*)

Challenge: shrink without shrinkage	Answer: don't trash but future-re-purpose
Estimated 200+ (granular) controls	Target: +/- 60 "wider-ranging" key controls
ICFR focus (RCM predominantly 1:1 relationships)	RCM review: bundle n risks : 1 control
Exhaustive documentation requirements	Consolidate over time (risk-based)
Strong (and equally exhaustive) ITGCs (&scope)	Narrow scope to ERP only (target IT scope)
Significant LoD 1, 2 and 3 involvement	Free up significant company resources
Additional efforts, such as 20-F disclosures, etc.	Largely to be discontinued (thorough assessment)

Control Framework downgrade-transitions call for "re-bundling" selectively for continued assurance

Short-Term Vision: the first twelve months to stabilize and optimize

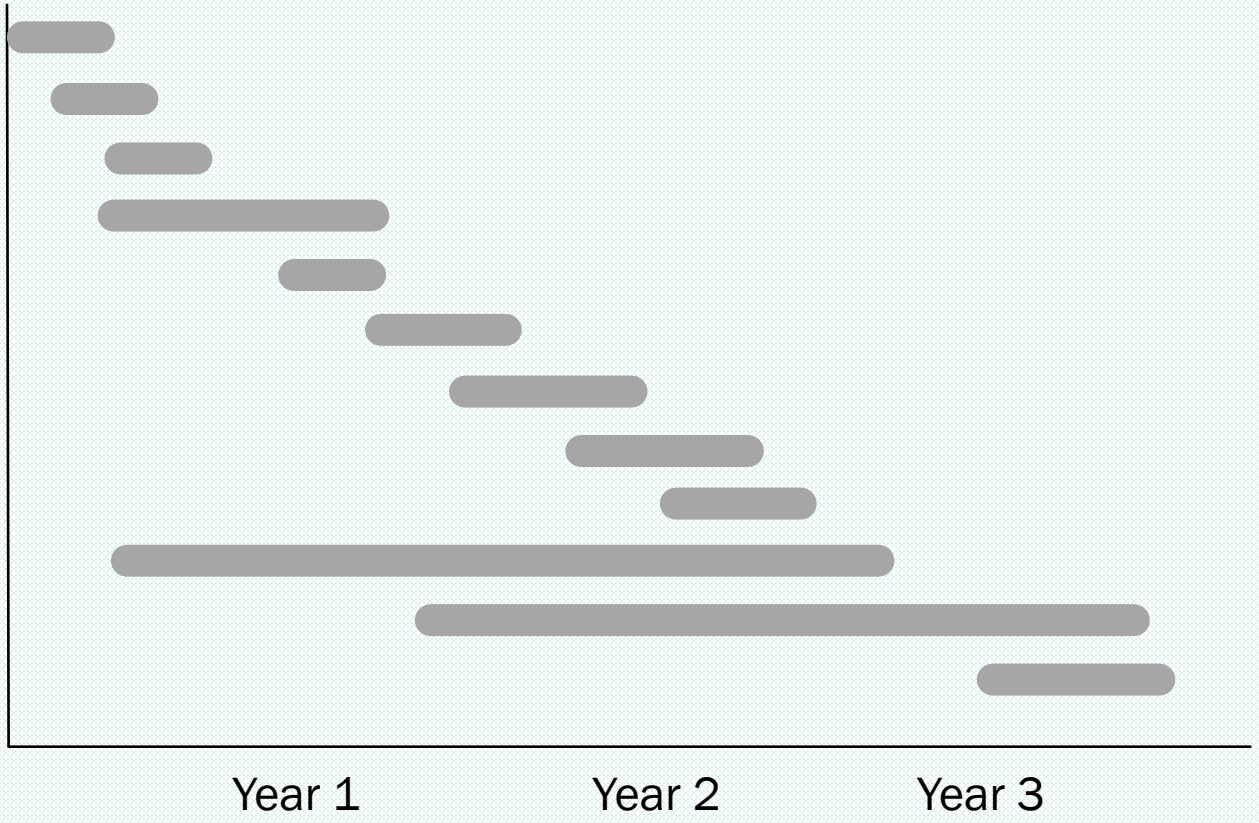
1. BoD/AC and Executive Management alignment
2. External Audit firm endorsement (universe, scope concept, plan)
3. Communicate on the LoD duties redistribution (content and staff impact)
4. Re-train (current) LoD 1, 2, 3 staff for new duties within functional/country organization
5. Nominate and appoint a diverse expert project group to “downgrade-transition” the ICFR framework
6. Initiate framework review and simplification exercise company-wide
7. Framework maintenance – no interim failures



Experience evidences in similar endeavors that solid foundations are of paramount important

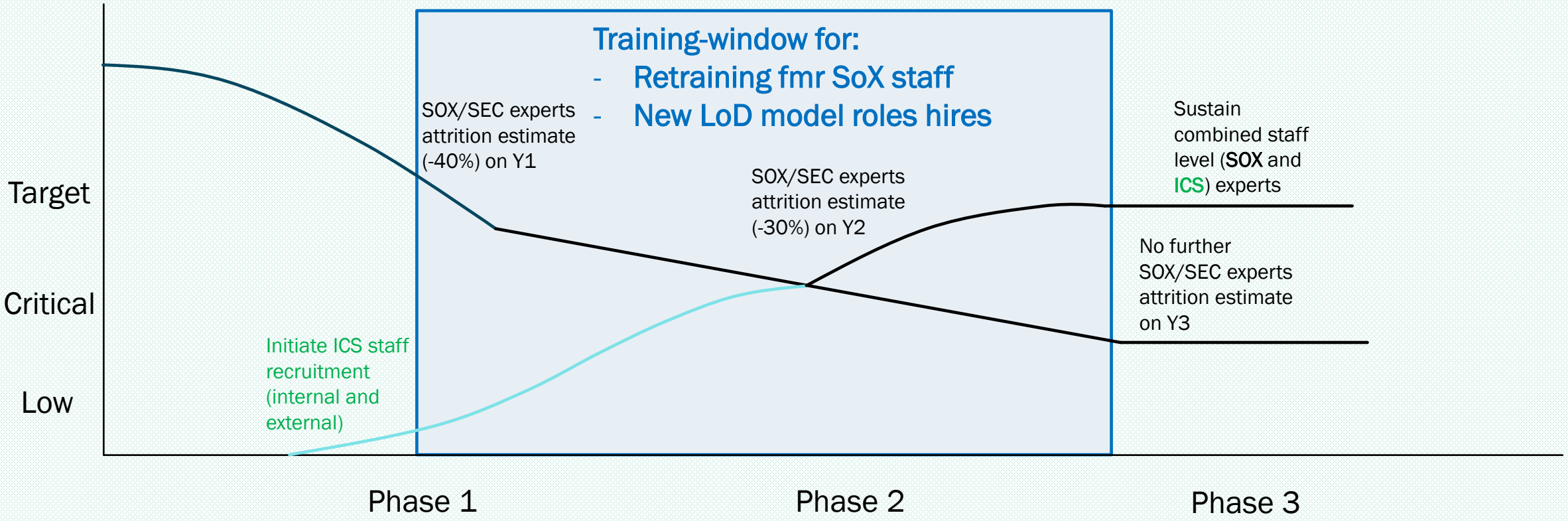
Medium to Long-Term Vision: (max.) three-year transformation roadmap

1. Validate (and DE test) reshaped framework
2. Gap-analyze that no significant risk unmitigated
3. Finalize first post-delisting framework
4. Trail-run framework controls
5. Make the framework “Audit-ready” first time
6. Validate obtained assurance with BoD/AC
7. Endorse attained simplification with Executives
8. Remediate any findings out of #6 and #7 above
9. Re-trail-run framework
10. Simulate “reliance agreement” testing with IA
11. Sustain and solidify – GRC IT strengthening
12. Reshape the LoD family of roles



Sustaining assurance: the amalgamation of buy-in, solidly reasonable content and state-of-the-art GRC IT

Leadership & Team Development: people at the core of success



Talent retention/development for the next ICS (&IA) leadership generation calls for company-wide planning

Leadership & Team Development: T&D specifics

Development group	Training & Development Measure
Former SOX experts ("old" LoD roles)	• On-the-job-training **beyond the confines of ICFR** (to acquire wider company process knowledge) complementing their expertise
Internal hires - diverse (to assume "new" LoD roles)	• ICS & IA academy training on Controls, Risk, Governance, Compliance with the aim to have the **broadest possible company functional representation** at ICS&IA roles
External hires	• **Target-role specific induction** training by ICS & IA academy
Executive Management (the talent pull-management group)	• Guidance on the **concept of using ICS & IA as the talent development center** of high potentials to assume a leadership position – estimated tenure of +/- 3 years at ICS & IA with the aim to staff tomorrow's leadership from WITHIN the Group.

Anticipation of attrition – timely and targeted training – and all for the great good of the company

Leadership & Team Development: Collaboration & Communication

Stakeholder	Approach (paradigm: walk the talk)
BoD and AC	• **Concise** – focus on assurance levels, respectively progress made to attain it • **Root cause remediation** of significant matters only • **Repeat findings** – elaborate on provenance and remediation suggestions
Executive Management	• Derive from BoD and AC materials (for **consistency and transparency**) • Root cause discussions with focus on **corrective actions and efficiency** gains • Increasingly elaborate on **GRC IT, simplification initiatives** and cost savings
Peers	• Exhaustive and **professional** amongst ICS & IA peers and other LoD roles • Clearly drive the ICS roadmap: **process and content** (though not without buy-in) • Ensure at all times they are (in fact and appearance) **part of the success story**
Staff to mid-senior level	• Focus on **what matters most** to this group: less bureaucracy and job security • Reinforce their **role's importance** in solid Governance • Continuously ensure (given that is true) **that no GRC initiative kills their job**

Own experience has shown that trustworthy professional communication at all levels is first priority

Conflict Management Approach: energy for growth

Conflict categories	Addressing the root cause	Using the item for growth
BoD/AC unsatisfied with "new" ICS framework exhaustiveness (and thus perceived assurance level)	Involving the Committee in closing alleged gaps; aim is to illustrate that there are none (fact vs appearance)	BoD/AC ICS "workshop" **to strengthen a firm trust in control substance** (vs. the light(er) appearance)
Executive Management unsatisfied with achieved level of simplification and residual "SOX bureaucracy"	Tackling the operational control performance metrics – hard and soft factors – to reflect leaner framework	Actively engage in rolling out the new ICS **control performance simplification project** (soft-factor: leave no staff level behind)
Any stakeholder unhappy with cost savings and synergies	Elaborate whether that is motivated by incentivization or budget constraints	Accelerate (vs. previous 3Y plan) the **deployment of GRC IT**
Delays in internal staffing for new ICS LoD roles	Illustrate that ICS & IA staff is NOT there to stay but to return to Business – enriched with expertise for higher duties	Build an **ICS & IA-talent pull-management environment** – use it as a talent development academy

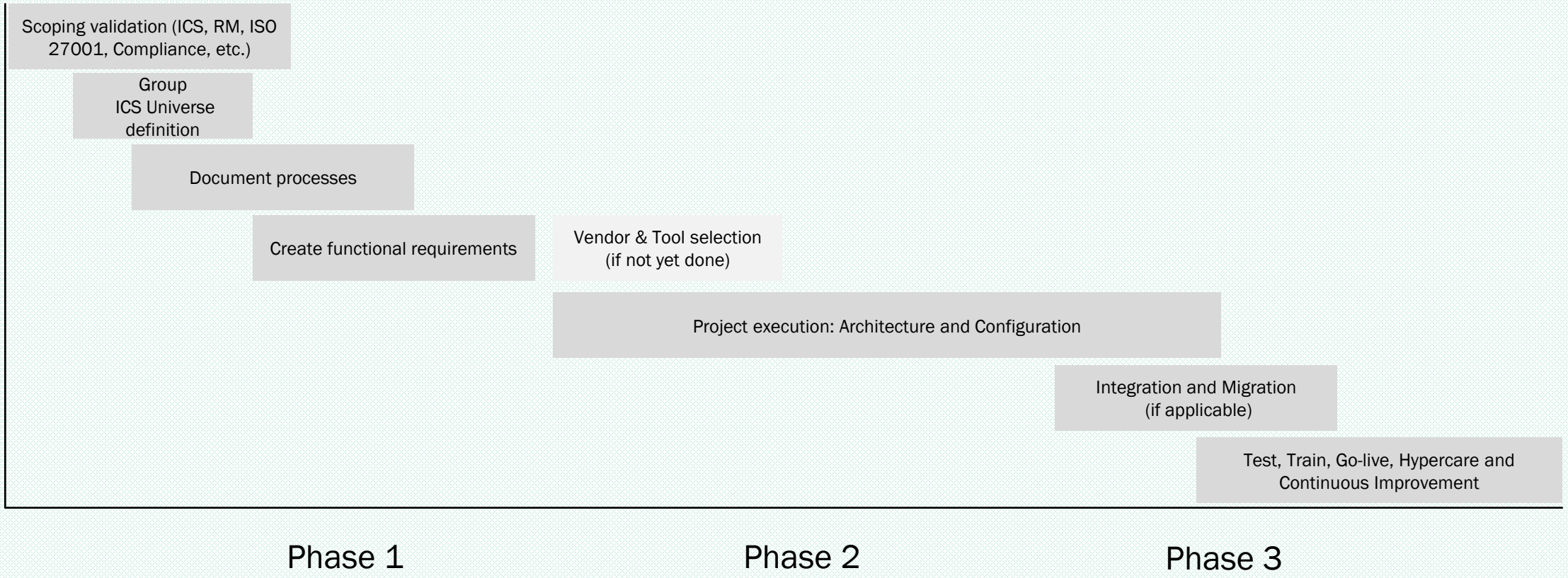
The conflict is the symptom, not the illness. Harvesting its energy for growth is art, not science.

Trade-Off Framework: minimizing compromises and losses

Trade-off element	Balancing consideration(s)	Envisaged resolution
Assurance level versus simplification (i.e. cost saving)	Finding the crossroads of maximum cost savings without substantial assurance loss	Review **exhaustiveness, scope and thresholds** of control narratives and evidence expectations
Manual framework duties versus GRC IT supported sophistication	For AI: drift and bias concerns For non-AI: control integrity vs manual performance	**Step-by-step digitization** (DEV, UAT, PROD) without any absolute target (paradigm: assurance quality first)
Internal Audit ICS effectiveness concerns versus its annual plan objectives	Internal Audit risk-based annual planning – scope and universe – reliance on ICS vs. LoD 1 and 2 controls	Shift GIA engagements from pre-delisting SOX environment **to functional LoD 1 and 2** reliance
Overall post-de-listing resistance versus remaining ICS compliance	The allowable "dropping the pen" phenomenon versus BoD/AC assurance level expectations	Communication, Conviction, Education and **"soft" but determined** ICS compliance enforcement

Resorting to a trade-off shall be the last consideration – compromises generate losses

Innovation & Digital Strategy: scalability through technology



GRC IT is of paramount importance to assurance scalability - requiring solid foundations

Innovation & Digital Strategy: a high-level look at technology

Automation potential:	Possible tool consideration:
• ULCM (User Life Cycle Management)	ServiceNow
• SoD (Segregation of Duties)	SAP GRC Access Control
• Key controls (ITGCs and Process Controls narratives)	Confluence
• Key controls (execution and evidence)	JIRA
• Process flowcharts library (including e.g. policy attachments)	SharePoint
• Financial closing process (controls, documentation, evidence)	FloQast

One of many automation benefits: from a culture of manual to system supported continuous monitoring

KPIs & Success Metrics: success through incentivization

Short-term (first year)	
KPI category	*Measurement*
BoD/AC concept approval	Within max 3 months
Management agreement	Within max 3 months
Staff attritions limits	No more than 30% in Y1
New experts recruitment	Within 6 months
All trainings completed	By latest end of Y1
GRC IT roadmap	Savings Forecast >20%

Mid- to Long-term (second, third year & beyond)	
KPI category	*Measurement*
Scope coverage	Functional & Org.
Control DE	% remediation
Control OE	% failure
Operational efficiency	Cost saving delta YoY
Assurance	% repeat findings
Audit (int. and ext.)	% impl. corr. actions

KPIs and Success Metrics to be tied to Incentivization schemes: quick-gains to be avoided unconditionally

Summary & Call to Action

First, foremost and above all: clear, unambiguous and transparent communication at all levels. Always!

Summary

1. Less control does not equal lower assurance
2. BoD/AC & Management expectations: no conflict
3. Do not underestimate the competency factor
4. Solid foundations are of paramount importance
5. Conflicts & Trade-offs to be anticipated
6. GRC IT cutting-edge for savings & effectiveness

Call to Action

1. >50% is credible “people-near” communication
2. Staff. Staff. Staff. Anticipate and be ready
3. Plan for conflicts and trade-offs: readiness
4. Emphasize the common and not the differences
5. Plan for each and communicate for all
6. Start early, very early, with GRC IT: synergies

(Swiss) ICS in a post-(US)delisting world: effective assurance can be achieved - even with less controls

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

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