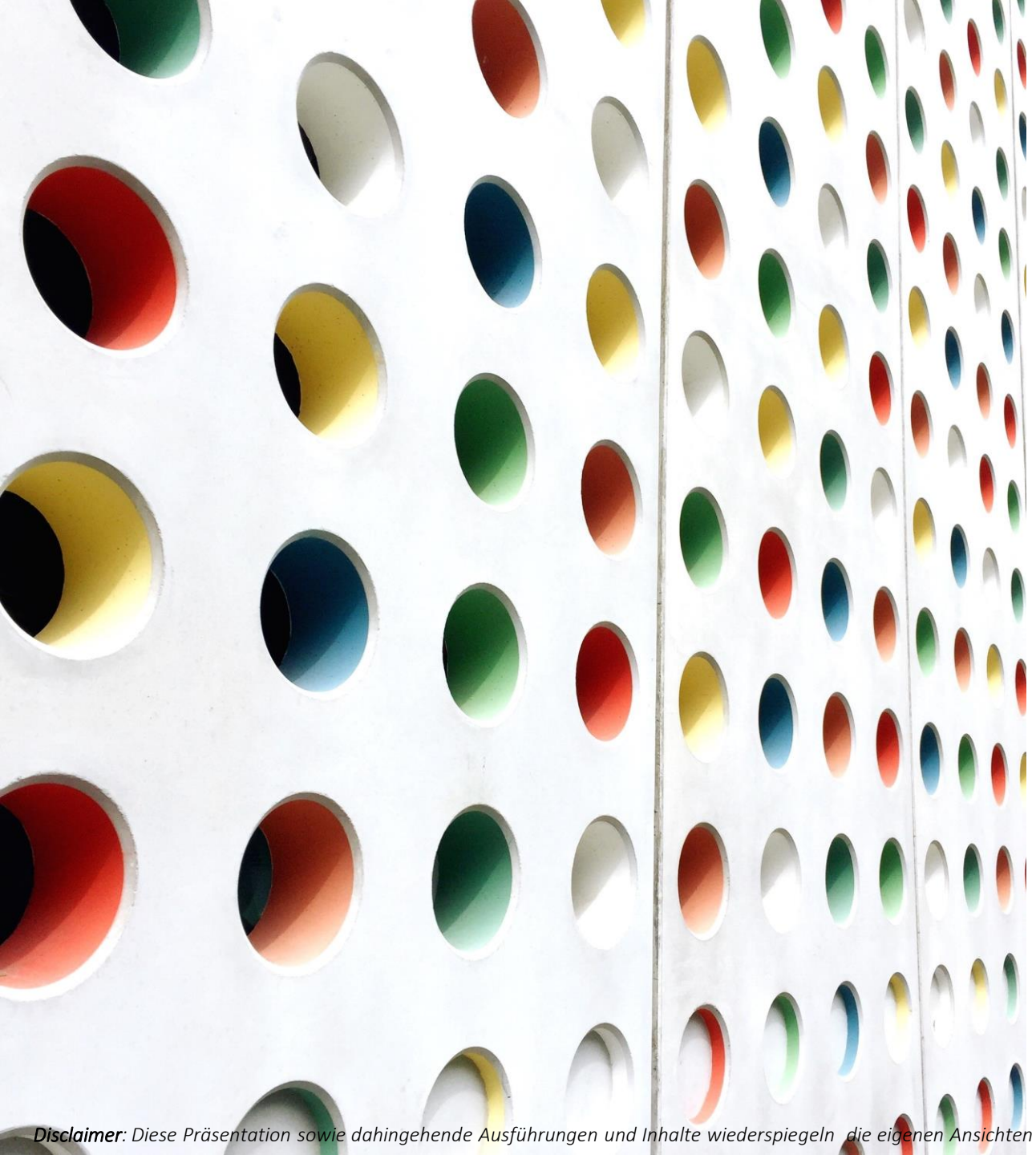


Aufbau eines ganzheitlichen IKS aus Risk- und Compliance Sicht

SWISS GRC DAY 2022

4. MAI 2022

EVA SEVERA-ZÜGER
(CCO ZURICH REINSURANCE COMPANY LTD)

SUSANNA LÜTHI-WALTER
(CRO ZURICH REINSURANCE COMPANY LTD)

Agenda

1. Einführung
2. Bausteine eines ganzheitlichen IKS
3. Herausforderungen & Erfolgsfaktoren
4. Fazit

Über uns

Susanna Lüthi-Walter

Lic oec. HSG / Dr. oec HSG

Über 10 Jahre (Aufbau)-Erfahrung im quantitativen und qualitativen Risiko-Management im Banken- und Versicherungsbereich, v.a.

- PostFinance (Senior Risk Manager)
- Helsana (Head Risk Management)
- Zürich Versicherung (Chief Risk Officer ZRe)

Independent Boardmember ab 1.1.2022

Herzblut Lehre

Eva Severa-Züger

Lic iur. HSG / LL.M. Lausanne

Über 10 Jahre Erfahrung im Bereich Legal, Compliance und Regulatory bei Versicherungen und Rückversicherungen:

- Partner Re (Legal Counsel)
- EY (Legal & Compliance Financial Services)
- Swiss Life (Legal & Portfolio Advisor)
- Zürich Versicherung (Compliance Officer Commercial Insurance, Chief Compliance Officer Zurich Reinsurance Company)

IKS: Entwicklung und Trend

Entwicklung

- Traditioneller Umfang des IKS: **Finanzberichterstattung** (vgl. Umsetzung Sarbanes Oxly Act (SOX), v.a. Section 404 und 302)
- «Internal Control» weist gemäss den anerkannten Rahmenwerken wie dem amerikanischen COSO («Committee of Sponsoring Organizations of the Treadway Commission»), dem kanadischen CoCo («Guidance on Control») oder dem britischen Turnbull eine **breitere Perspektive** auf als diejenige von Section 302 und 404 des SOX. Die Rahmenwerke beziehen neben den im SOX fokussierten Massnahmen für eine zuverlässige Berichterstattung auch die beiden weiteren Zielkategorien Wirksamkeit und Effizienz der Geschäftstätigkeit und Compliance mit Gesetzen und Normen vollständig mit ein.

- Anforderung aus dem Obligationenrecht (OR 728a und 728b) fordern ein **funktionsfähiges Internes Kontrollsystem**.
- **Regulatorische Anforderungen** für Finanzinstitute (z.B. FINMA Rundschreiben 2008/21; FINMA Rundschreiben 2017/2 Corporate Governance - Versicherer, Bankgesetz (BankG) und Börsengesetz (BEHG)).

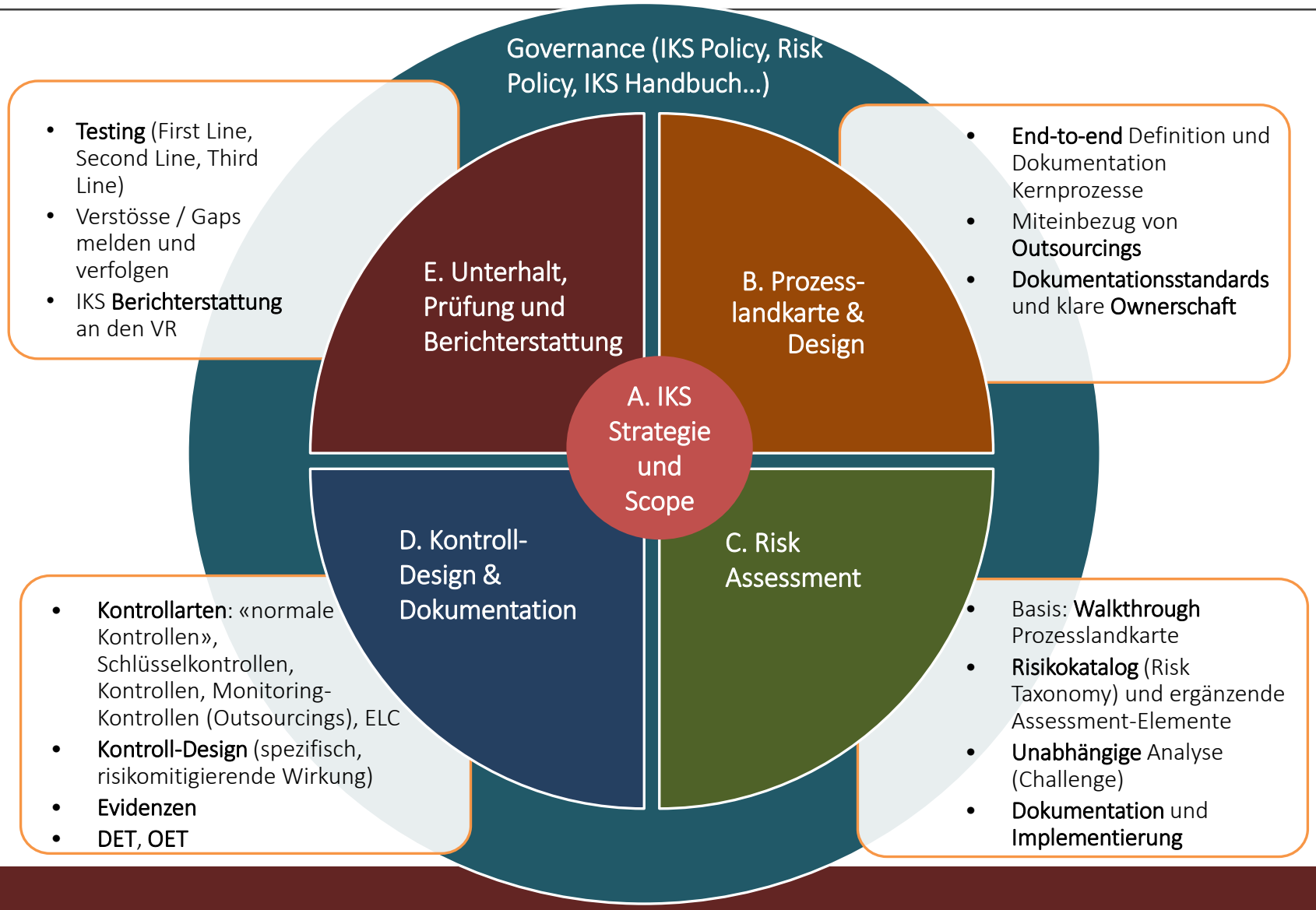
Trend

- **IKS** und Enterprise Risk Management System (ERM) im **Fokus** der **Corporate Governance Diskussion: Überwachungssysteme** gewinnen gerade im heutigen Umfeld (u.a. hohe Regulierungsdichte, komplexe Unternehmensprozesse) an Bedeutung.
- **Ganzheitliches IKS:** Integraler Bestandteil des unternehmensweiten Risikomanagement, welches alle wesentlichen **operativen** und **finanziellen** Unternehmensrisiken abbildet und auf ein für das Unternehmen tragbares Niveau reduziert. => **Einbindung** von **Compliance Risiken**.
- **Präventive und aufdeckende Funktion**; Unterstützung des Ablaufes der Unternehmensprozesse.
- **Digitalisierung** (Verwendung von IT-Tools zur Dokumentation des IKS, die von allen 3-Lines of Defence genutzt und verstanden werden und auch Massnahmenpläne verbindlich abbilden können).
- Bestehende Strukturen vereinfachen und optimieren **(make it simpler and better).**

Agenda

1. Einführung
2. Bausteine eines ganzheitlichen IKS
3. Herausforderungen & Erfolgsfaktoren
4. Fazit

Bausteine eines ganzheitlichen IKS



A. IKS Strategie und Scope

Hintergrund
- Der Verwaltungsrat hat die Oberaufsicht über das IKS.
- Seitens der Best-Practice wird erwartet, dass hierzu eine Strategie festgelegt wird (ICS-Questionnaire FINMA, Rundschreiben etc.)

Strategie
- Die IKS-Strategie soll den **Ambitionslevel** (I. Initial, II. Repeatable, III. Defined, IV. Managed and Monitored) festlegen und ist durch den Verwaltungsrat zu genehmigen.
- Ebenfalls sollte regelmässig (mindestens jährlich) bestimmt werden, welches Maturitätslevel das IKS erreicht (IST- Einschätzung). Dabei soll die adäquate Ressourcenausstattung IMMER in diese Analyse miteinbezogen werden, wenn es um die Definition des Ambitionslevels geht.
- Die Ist-Analyse des Maturitätslevels des IKS ist in die Berichterstattung an den Verwaltungsrat zu integrieren. Dabei ist es wichtig, dass dem Verwaltungsrat eine **Integrated Assurance-Sicht** geboten werden kann (Risk, Compliance, Audit).

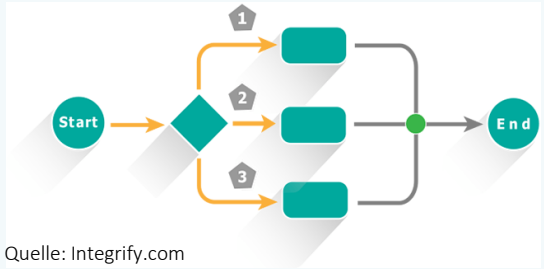
Scope
- Der Scope des IKS kann entweder risikobasiert (risikoreiche und kritische Prozesse aus Risk- oder Compliance Sicht) oder aber aufgrund des z.B. Bilanzvolumens definiert werden.
- Dadurch wird klar, welche Prozesse im Folgejahr im Fokus stehen. Ein begründetes Roll-out hilft, Planungstask frühzeitig zu initiieren.

Dokumentation
- Der Umfang des IKS wird in den internen Weisungen und Handbücher dokumentiert (Risk Policy, IKS Policy, IKS Handbuch)

B. Prozesslandkarte & Design

Kernelemente aus Risk Sicht (bisher)

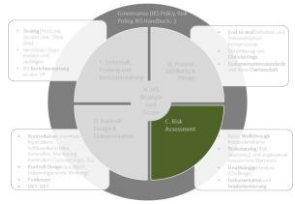
- Prozesse sowie mögl. Subprozesse müssen die Wertschöpfung wiederspiegeln (Primär-/Sekundärprozesse) → **end-to-end**
- Allfällige **Outsourcings** müssen klar aufgezeigt werden
- Die Definition von minimalen **Prozessdokumentationsstandards** hilft, einen einheitlichen Ansatz zu etablieren (i.e. beteiligte Parteien und Tasks, Schnittstellen-Tasks etc.)
- Die Prozessbeschreibung muss für einen unabhängigen Dritten **nachvollziehbar** sein und…
- …in adäquaten Abständen **aufdatiert** werden
- Die Dokumentation bietet die Grundlage für ein erfolgreiches **Risk Assessment**



Quelle: Integrify.com

Kernelemente aus Compliance Sicht (ergänzend)

- Bestimmung der Prozess-Owner in der First Line
- Compliance Risiken müssen mittels angemessener Prinzipien, **Prozessen** und Kontrollen mitigiert werden
- Chance für Compliance, sich mit den Kern-Prozessen des Unternehmens vertraut zu machen und die Unternehmensabläufe besser zu **verstehen**
- **Aktualisierung** der Prozesse bei Änderungen (z.B. Änderungen der internen und externen Anforderungen)



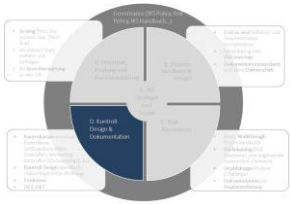
C. Risk Assessment (Risikokatalog)

Kernelemente aus Risk Sicht (bisher)

- Basierend auf dem Prozessbeschrieb und einem «**Walkthrough**» kann ein Assessment stattfinden
- Ideal gibt es dafür zentrale **Risikokataloge (Risk Taxonomy)**. Wenn nicht, kann man sich taylor-made für das Geschäftsmodell selber einen solchen kreieren (Basis z.B. Rundschreiben 2008/21 Operationelle Risiken Banken Anhang 2)
- **Ergänzende Assessment-Elemente** sollen herangezogen werden
  - Findings Audit, 2nd-line oder Regulator
  - OEMs
  - BCM-Szenarien
  - Bisher erfasste Risiken und deren Adäquanz
  - Veränderte interne- und/oder externe Anforderungen etc.
- Der **Prozessowner** sowie (unabhängig) der **Risk Officer** analysieren welche der Risiken gemäss Risk Taxonomy in scope sind
- Die assessten Risiken (Outcome) werden konsolidiert **dokumentiert** und von allen Beteiligten (Prozess-Owner, Risk Officer, Compliance Officer) unterzeichnet und im Prozess dokumentiert
- Allfällige GAPS oder Empfehlungen werden mit Ownern und Due-dates versehen
- Deren Implementierung wird überwacht

Kernelemente aus Compliance Sicht (ergänzend)

- **Inventar**: Erstellen eines **Compliance Risiko Inventars** aufgrund der anwendbaren wesentlichen **internen und externen Anforderungen** (optimalerweise ist dies Teil des Gesamt-Risiko Inventars).
  - ➢ Welche wesentlichen rechtlichen und regulatorischen Anforderungen sind anwendbar? (Rechtliches Inventar erstellen)
  - ➢ Welche Anforderungen aus internen Weisungen gibt es?
- **Verlinkung**: Compliance Risiken werden mit den Prozess-Ownern besprochen, mit den Prozessen verlinkt und Compliance Officer gechallenged.
  - ➢ Wo schlagen sich die Compliance Risiken im Prozess nieder?
  - ➢ Wie werden Risiken verlinkt, die für mehrere Prozesse anwendbar sind?
- **Ausgliederung**: Risiken können nicht an Service Provider «ausgegliedert» werden
- **Rechtsentwicklung**: Änderungen der internen und externen Anforderungen müssen überwacht und analysiert werden.
  - ➢ Sind Anpassungen im Compliance Risiko Inventar, bei den Prozessen und Kontrollen notwendig bei Änderungen?



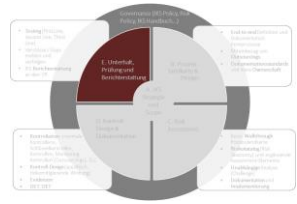
D. Kontroll-Design & Dokumentation

Kernelemente aus Risk Sicht (bisher)

- Basierend auf dem **Risikokatalog (Risk Taxonomy)** werden Kontrollen lokal adaptiert
  - «normale Kontrollen»
  - Schlüsselkontrollen
  - Monitoring Kontrollen (für **Outsourcings)**
  - Entity-Level Controls
- Vorgabe des **Kontroll-Design** (why, what, how, when, who) für verständliche und einheitliche Kontrollen
  - Dabei muss sichergestellt werden, dass die **Formulierung** der Kontrolle auf die Risiko(teil)mitigierung zielt. Bestehen bereits Mitigierungaktionen (zB Standardagenda) kann dies dokumentiert werden (braucht evt keine Kontrolle)
  - **Effizienzgewinn** durch gute (spezifische aber breite) Formulierung einer Kontrolle, die durch denselben Owner durchführt wird (1 Kontrolle, die mehrere Risiken migriert)
- Weiter muss der **Bestätigungszyklus** (YoY, QoQ o.a.) hinterlegt werden sowie…
- … die Definition von erwarteten **Evidenzen** zwecks Kontrolldokumentation
- Der Kontroll-Owner soll jeweils in einem Zyklus selbst assessen, ob seine **Kontrolle effektiv** ist (DET, OET)
- Die **Segregation of Duties** ist jederzeit zu beachten

Kernelemente aus Compliance Sicht (ergänzend)

- Evaluierung wie Compliance Risiken mittels **wirksamen Kontrollen** verhindert/ reduziert werden können (welche Kontrollen sind bereits vorhanden, welche sind notwendig?)
- **Bestimmung von Kontroll-Zielen** innerhalb des Unternehmens für ein einheitliches Risiko und Kontroll-Management
- **Dokumentation:** Verlinkung der Compliance Risiken mit Kontrollen zur Verhinderung oder Reduzierung der Compliance Risiken
- Anpassung der Kontrollen infolge Änderungen der internen und externen **Anforderungen**
- Wichtig bei Ausgliederung: **Outsourcing** Monitoring Kontrollen zur Überwachung der ausgegliederten Dienstleistung
- Auch Compliance Kontrollen sollten durch die **First Line** ausgeführt werden (First Line ist Owner der Compliance Risiken)



E. Unterhalt, Prüfung und Berichterstattung

Kernelemente aus Risk Sicht (bisher)

- Es soll ein **risikobasiertes Testing** aufgegleist werden…
- Dabei braucht es ein **Testing-Konzept** (Roll-out Prozesses, Fokus auf gewisse Risiken und Kontrollen, Roles and Responsibilities)
- Dieses soll auch mit den anderen **Assurance-Functions** aligned werden (no testing on work-in-progress)
- Auch hier gilt es, die **Segregation of Duties** zu beachten und …
- …dem Management den **Mehraufwand** bewusst machen (Ressourcen)
- Jährliche **Berichterstattung** an den Verwaltungsrat

Kernelemente aus Compliance Sicht (ergänzend)

- **Design** und **operationelle** Effektivität der Kontrollen testen (risikobasiert, durch alle drei Linien der Verteidigung).
- Durchführen eines jährliches **Compliance Risk Assessments**, welches auch die Beurteilung der Kontrollen zur Reduzierung der Compliance Risiken beinhaltet.
- Jährliche Beurteilung der **Angemessenheit** der Prinzipien, Prozesse und Kontrollen zur Einhaltung der internen und rechtlichen Anforderungen (Maturitäts-Analyse).

Agenda

1. Einführung
2. Bausteine eines ganzheitlichen IKS
3. Herausforderungen & Erfolgsfaktoren
4. Fazit

Herausforderung: Integrativer aber pragmatischer Ansatz (1/2)

Herausforderungen		Erfolgsfaktoren
Komplexität, Unterhalt und Nutzen	• IKS ein komplexes, sehr **arbeitsintensives** Thema • Heute ist IKS immer noch vielfach eine "**tick-the-box**" Übung und ist nicht mit dem Riskmanagement verzahnt • Oft unklar, wo die **IKS-Fachstelle** angesiedelt werden soll (1st-Line/2nd-Line) • **Ressourcenknappheit**	• **Nutzen** aufzeigen (gut gemanaged erleichtert IKS das Business) • Fokus auf **Kernelemente** (Key-Risk, Key-Control) • **Ressourcenallokation** in 1st-Line UND 2nd-Line • IKS Verantwortliche in der First Line
IKS-Strategie und Scope	• IKS Strategie und Ziel ist unklar • Veränderungen werden nicht von heute auf morgen erzielt und brauchen **Zeit**	• Der **Maturitäts-level** sollte klar bestimmt sein (Risikoappetit) • Klare Darstellung Ist-Soll (Verwaltungsrat) • Gap in eine **Roadmap** verpacken und Ressourcen sicherstellen • Risk & Compliance als unabhängiger Supporter
Prozesslandkarte	• Oft sind Prozesse nicht oder nicht klar **beschrieben** (Basis Risikoidentifikation) • Dazu gehören auch **Outsourcings** (Third-Party), denn das Risiko verbleibt lokal und muss gemanaged werden • Risiken und Kontrollen müssen zu Prozessen **verlinkt** werden	• Prozesse sollten **pragmatisch** dokumentiert sein (Visio/Word) • **Verantwortlichkeiten** müssen klar geregelt sein (Ansprechpartner) • **Schnittstellen** zu Service Provider aufzeigen
Risikoidentifikation	• Oftmals werden Wirkungen und nicht **Ursachen** beschrieben • Miteinbezug der **Emerging Risks** • Einstufung v.a. der Operativen Risiken ist keine exakte Wissenschaft und basiert immer auf **Expertenwissen** (Brutto/Nettosicht) • Miteinbezug von **Compliance-Risiken** aber auch **IT-Risiken** immer wichtiger • **Frühwarnindikatoren** (KPI) (Trigger)	• Vulnerability-Trigger-Consequence • **What keeps you awake at night** (Risk-Assessment) • Berücksichtigung **Third-Party-Risks** • Kategorisierung inkl. Risikostrategie • Klare **Owner**

Herausforderung: Integrativer aber pragmatischer Ansatz (2/2)

Herausforderungen		Erfolgsfaktoren
Kontrolldesign	• Oftmals sind Kontrollen einfach «**tick-the-box**» Übungen: zu viele Kontrollen /wenig Sinn (Design Effectiveness) • Kontrollen sind oft zu **wenig klar** formuliert (z.B. fehlende Angaben zu Häufigkeit, Owner, Kontrollaktivität, nicht risikomitigierend) • **Evidenzen** oftmals nicht gut genug (Operative Effectiveness)	• Fokus auf **Key-Controls** (Key-Risks) • **Recycling** und Mehrfachnutzung • **Verzahnung** zum Risiko inkl. -strategie (Kontrolle sollte das Risiko reduzieren/mitigieren) und den Vorgabedokumenten • Aufzeigen, welche **Kernelemente** zu einer guten Kontrolle gehören • Arbeiten mit **Beispielen** (Schulung) • Einbau von erleichternden **Steuerungselementen** im Tagesgeschäft (z.B. Standard-Agenda item, Geschicktes Aufsetzen von Vorgabedokumente) • **Aktives Einfordern** von Evidenzen • Einheitlicher Ansatz im Unternehmen (Vorgabe von **Minimalanforderungen** zum Kontroll-Design) • **Selfassessment** DET / OET

Agenda

1. Einführung
2. Bausteine eines ganzheitlichen IKS
3. Herausforderungen & Erfolgsfaktoren
4. Fazit

Fazit

Für ein ganzheitliches IKS aus Sicht Risk- und Compliance braucht es:

- Einen **pragmatischen** Ansatz, der der 1st-Line **Nutzen** stiftet
- Eine integrative und abgestimmte **IKS-Strategie** und – Umsetzungsplanung

- Eine «**end-to-end**» Prozess-Dokumentation (inkl. **Outsourcings**) sowie zugrundeliegende **Vorgabedokumente**

- Ganzheitliches Assessment über **lokale Risiken** inklusive **Compliance-Risiken**, mögliche **Mitigierungsmassnahmen** und **Kontrollen** (2nd-line als Challenger)
- Abgestimmte **Instrumente, Tools** und **Berichterstattung** zwischen Risikomanagement und Compliance

- Genügend **Ressourcen** und starke **Einbindung** der First Line

Disclaimer: *Diese Präsentation sowie dahingehende Ausführungen und Inhalte wiederspiegeln die eigenen Ansichten der Vortragenden wieder und nicht diejenige von Zurich Versicherung.*

Questions?