ISSX IT-Security Swiss Conference

VOGEL IT AKADEMIE

www.issxconference.ch

#issxconference

ISSX

Vom Fragebogen-Friedhof zur gezielten Steuerung: Praxiserfahrungen einer risikobasierten TPRM-Triage

Pfäffikon SZ, 30.06.2026

Referent

Bruno Blumenthal

Dipl. Ing. FH in Informatik, CISM, CISA, CISSP
Partner, Mitglied der Geschäftsleitung TEMET AG

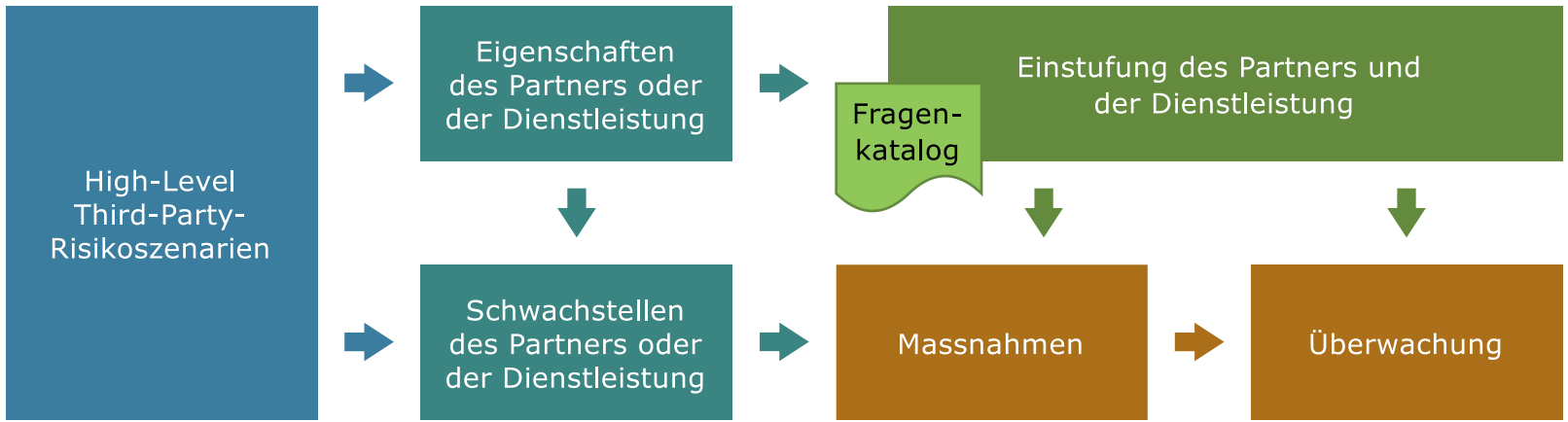
Spezialgebiete:

- Information Security Management Systems (ISMS)
- Cyber Risk Management
- Security Architecture & Strategy
- Cybersecurity & Security Operations

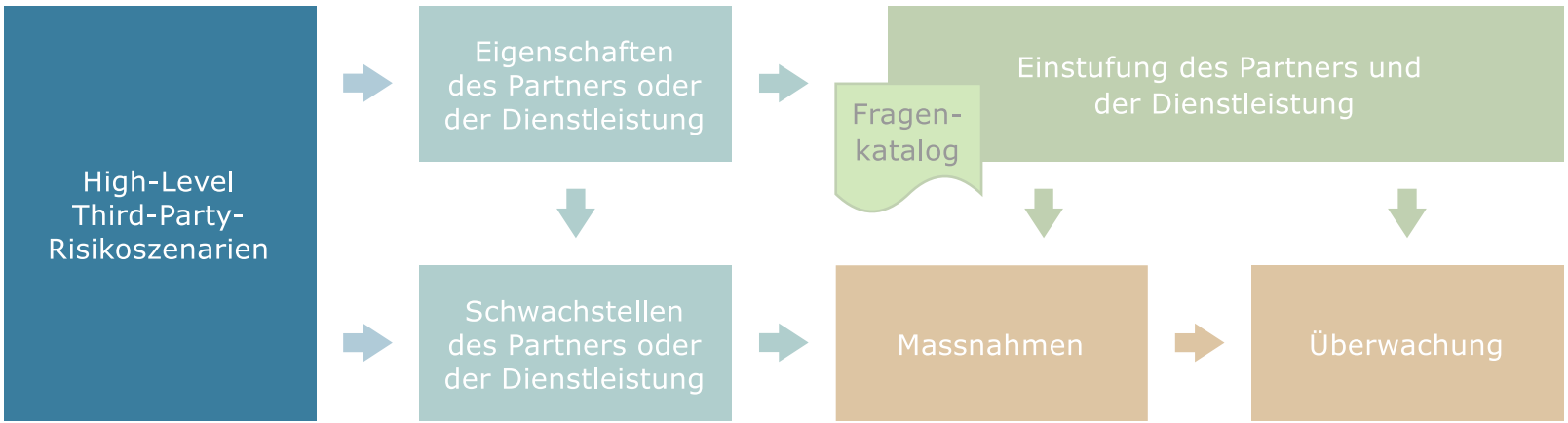
Kontakt:

Mobile: +41 78 859 57 15
E-Mail: bruno.blumenthal@temet.ch

Ein TPRM-Framework



High-Level Thrid-Party-Risikoszenarien



Risikokategorien

Funktionalität

- Unzureichende Sicherheitsfunktionen
- Fehlende Integrierbarkeit
- Risikobehaftete Funktionalitäten

Qualitätsmängel

- Sicherheitsschwachstellen in der Lösung
- Unzureichende Informationen
- Nicht adressierbare Schwachstellen

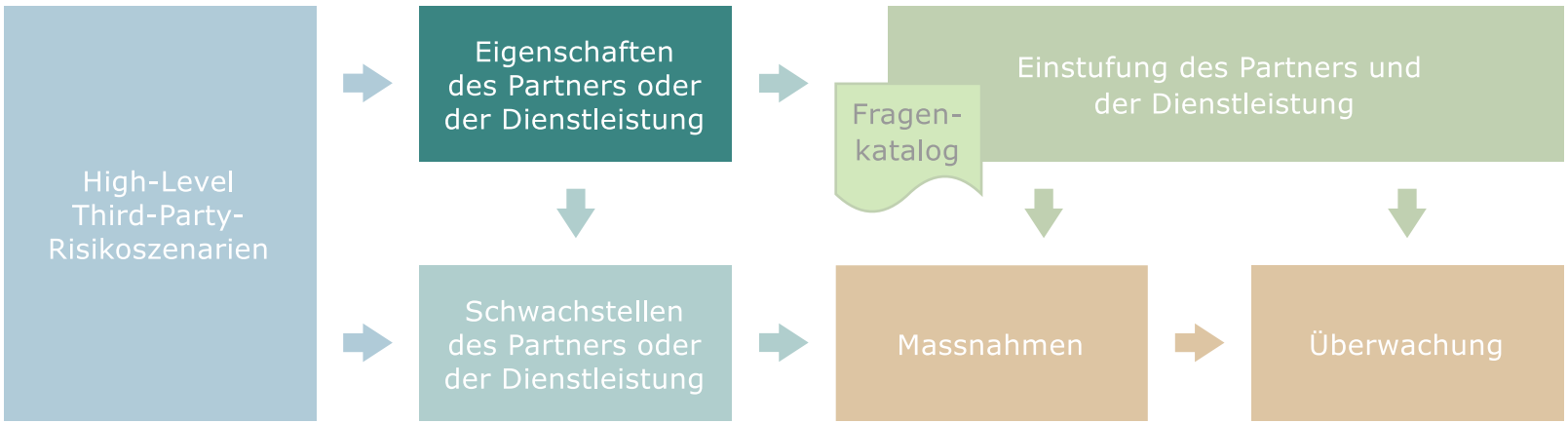
Kompromittierung

- Eingeschränkte Lieferfähigkeit
- Datenabfluss bei der Third-Party
- Third-Party als Einfallstor

Missbrauch des Zugriffs

- Remote-Access-Risiken
- Lokaler Zugriff durch Dritte
- Unautorisierter Datenzugriff beim Dritten

Firmen- und Dienstleistungseigenschaften



Firmen- und Dienstleistungseigenschaften

Dienstleistungsart

- Software
- IT-Services
- Dienstleistungen
- Maschinen
- Rohmaterial

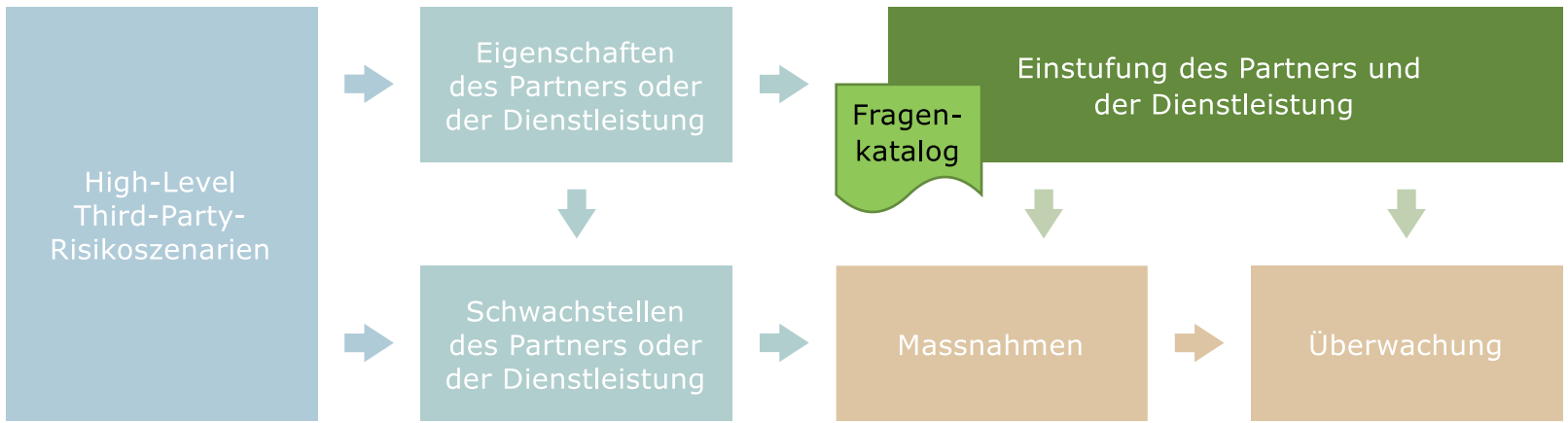
Business-Relevanz

- Prozesskritikalität
- BIA-Einstufung
- Abhängigkeiten

Schutzbedarf

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Datenschutz
- Regulierte Daten

Einstufung

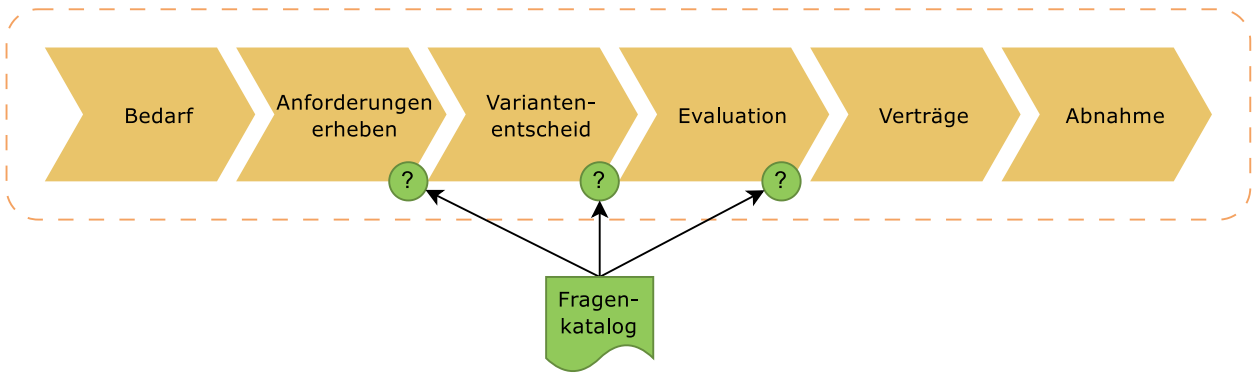


Fragenkatalog – One Size Doesn’t Fit All

- Wie gehe ich mit mehreren tausend Lieferanten um?
- Alle gleich zu behandeln ist unmöglich.
- Ein zentraler Schritt ist daher die Relevanzeinstufung.
- Als Grundlage dafür dienen die Firmen- und Dienstleistungseigenschaften.
- Die Einstufung steuert
  - die initiale Triage,
  - die Auswahl passender Massnahmen sowie
  - die Definition der kontinuierlichen Überwachung.

Integration in die Organisation

- Wie bette ich die Einstufung in bestehende Prozesse ein?
- Zu welchem Zeitpunkt liegen alle benötigten Informationen vor?
- Wie halte ich die Einstufung dauerhaft aktuell?

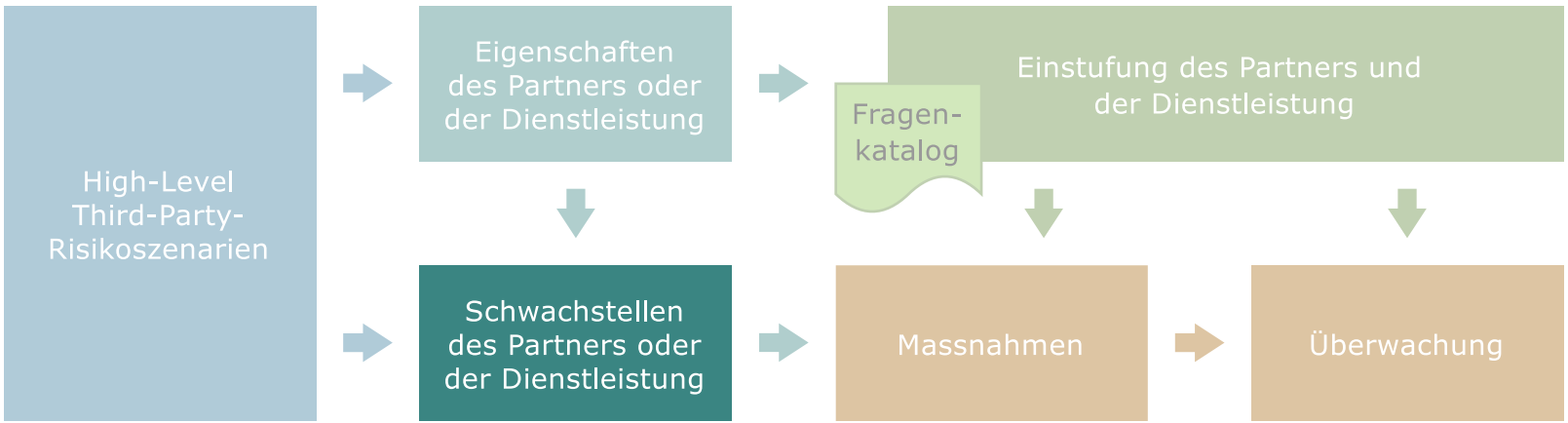


Herausforderungen

- **Dezentrale Beschaffung**
  - Shadow-IT und unregulierte SaaS-Nutzung
  - Beschaffungsprozesse ohne direkten IT-Bezug
- **Kleine Änderungen (Changes) ausserhalb von Projekten**
  - Lifecycle-Management
  - Funktionale Software-Änderungen
  - Hardware-Replacements
- **Fusionen & Übernahmen (M&A) bei Lieferanten**

Ein TPM und eine hohe allgemeine Prozessmaturität sind der Schlüssel zum Erfolg.

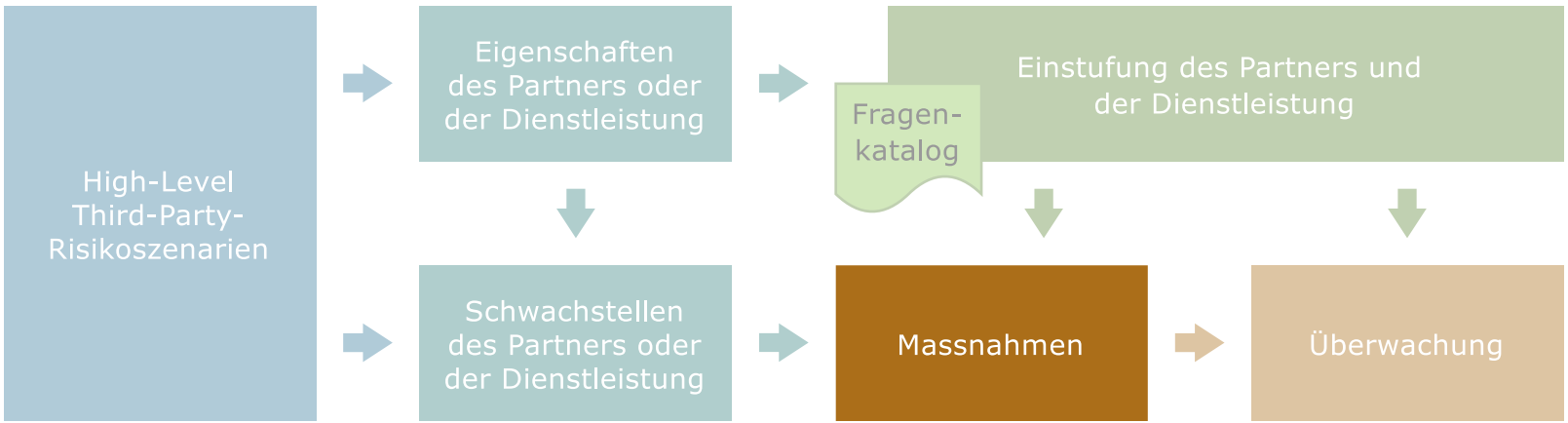
Schwachstellen des Partners oder der Dienstleistung



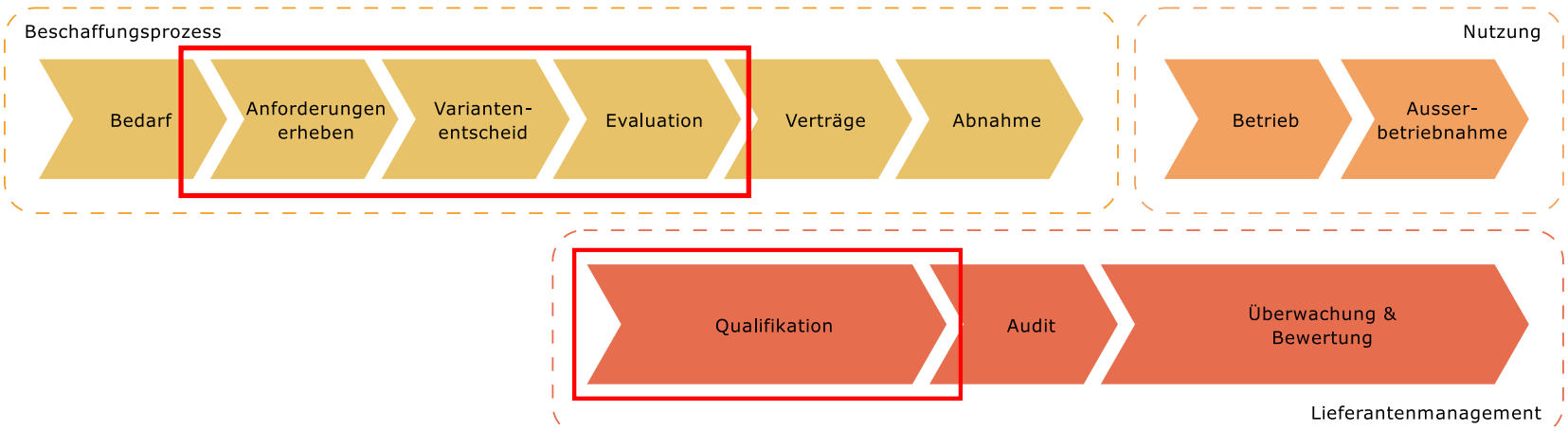
Schwachstellen des Partners oder der Dienstleistung

- Mangelndes Sicherheitsmanagement
- Unzureichendes Business Continuity Management (BCM)
- Fehlende Sicherheit im Software Development Life Cycle (SDLC)
- Mangelhafter Incident-Response-Prozess
- Undefinierter Informationsfluss bei Vorfällen
- Fehlende Sicherheitskultur
- Unzureichendes eigenes TPRM des Dienstleisters

Massnahmen



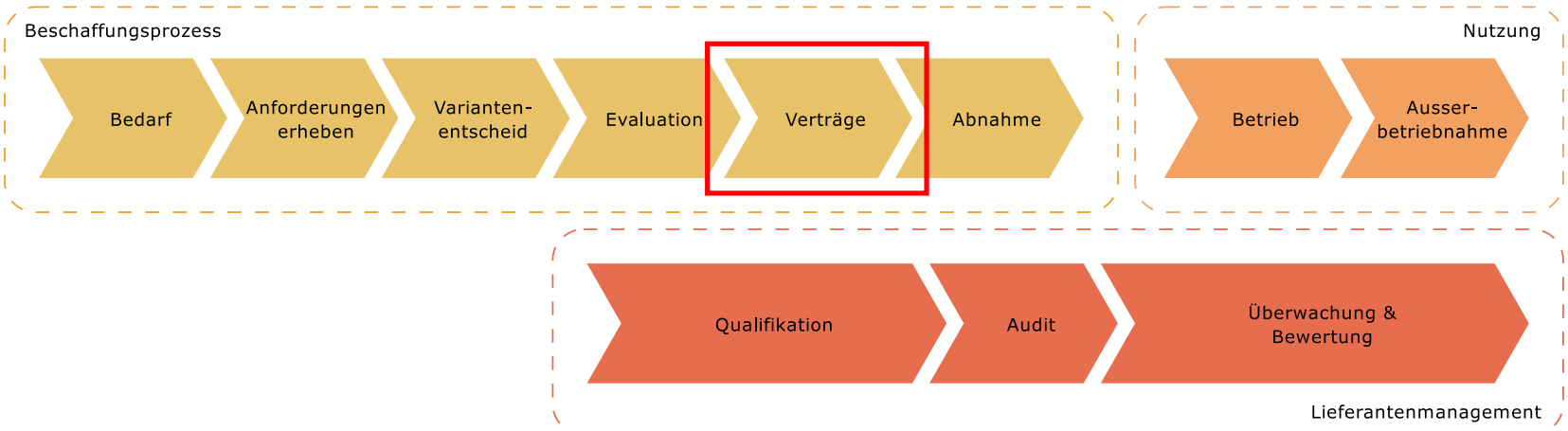
Massnahmen: Anforderungen



Anforderungen

Firmen Anforderungen	Generische Anforderungen	Spezifische Anforderungen
Allgemeine Anforderungen an den Lieferanten: • Interne Organisation und Sicherheitsmanagement • Organisatorische Schnittstellen und Ansprechpartner • Umgang mit Schwachstellen und Incidents	Technischer Grundschutz: • Generelle Technologie-anforderungen für die Integration • Basissicherheitanforderungen basierend auf der Technologie und Einsatzzweck	Spezifische technische Anforderungen an das konkrete Beschaffungsobjekt: • Vollständig neue, individuell definierte Anforderungen • Aus den Anforderungen abgeleitete und konkretisierte Anforderungen
Beschaffung	Projektmanagement	

Massnahmen: Verträge



Verträge: Gemeinsames Verständnis

Erwartungsmanagement

- Cybersecurity wird oft implizit vorausgesetzt,
- in der Praxis jedoch selten im erwarteten Mass geliefert.

Anforderungen verbindlich festhalten

- Kriterien aus der Evaluation müssen vertraglich fixiert werden.
- Die vertragliche Vereinbarung bildet die rechtliche Grundlage für die spätere Überwachung.

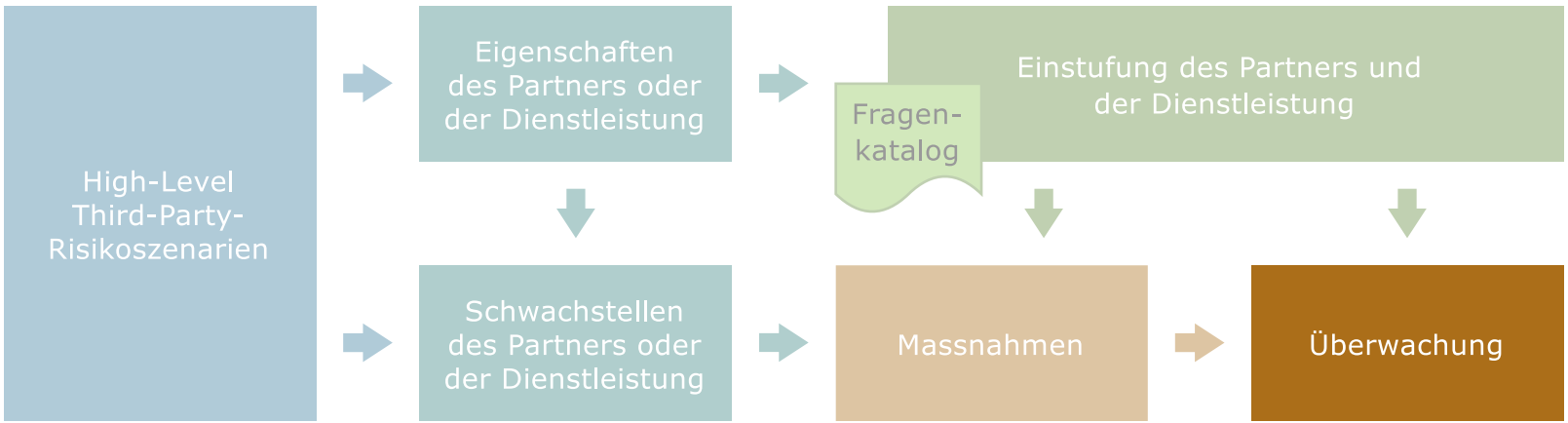
Scoping (Abgrenzung)

- Die Anwendbarkeit der Sicherheitsklauseln muss eindeutig geregelt sein.
- Sind beispielsweise auch reine Projektmanagement- oder HR-Systeme im Scope?

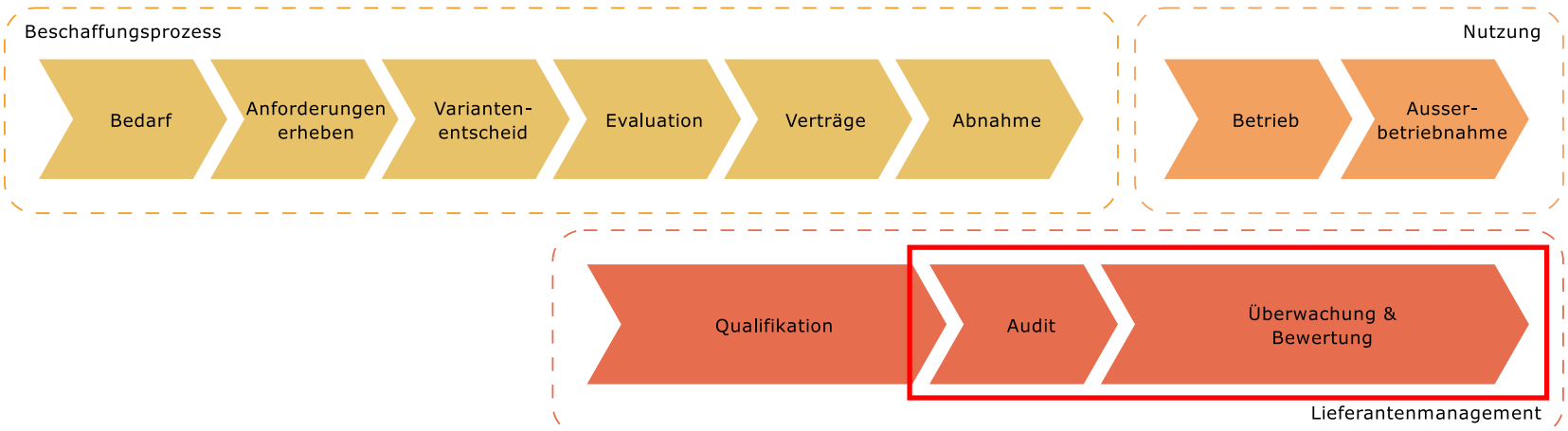
Verträge: Inhalte

- Der Lieferant verfügt über ein angemessenes Managementsystem für Cyber-Risiken.
- Die Mitarbeitenden des Lieferanten werden regelmässig bezüglich Cyber-Risiken sensibilisiert und geschult.
- Cybersecurity ist integraler Bestandteil der Entwicklungs- und Wartungsprozesse.
- Der Lieferant verfügt über etablierte Prozesse zur Meldung und Behebung von Schwachstellen.
- Die Zusammenarbeit im Falle eines Cybervorfalls ist klar geregelt.
- Der Lieferant ist verpflichtet, diese Sicherheitsanforderungen an seine eigenen Subunternehmer weiterzugeben.
- Der Lieferant räumt dem Kunden Möglichkeiten ein, die Einhaltung der vertraglichen Pflichten zu überprüfen.

Überwachung



Audits und Überwachung



Mittel der Überwachung

Individuelle Audits

Der Kunde führt selbstständig oder durch Beauftragte ein Audit beim Lieferanten durch.

Zertifizierungen

Der Lieferant weist die Compliance durch die Zertifizierung nach einem anerkannten Standard nach.

Assurance-Reports

Unabhängige Dritte bestätigen die wirksame Umsetzung definierter Kontrollen (Controls).

Right-to-Audit

Grundlage

- Eine Standardklausel in vielen Dienstleistungsverträgen.
- Ein klassisches Instrument der Lieferantenüberwachung.
- Die Überprüfung erfolgt direkt durch den Kunden oder einen beauftragten Dritten.

Herausforderungen

- Häufig vertraglich vereinbart, aber in der Praxis selten genutzt.
- Hoher personeller und zeitlicher Aufwand für Kunde und Lieferant.
- Die Kostenaufteilung muss vorab eindeutig geregelt sein.
- Der genaue Prüfumfang (Scoping) der Audits ist oft unklar.

ISO/IEC 27001-Zertifizierungen

Der Standard

- Der weltweit führende Standard für Informationssicherheits-Managementsysteme (ISMS).
- Der Fokus liegt primär auf Prozessen, Dokumentation und Vorgaben.

Das Problem

- Zertifikate gelten oft nur für spezifische Teile oder Standorte des Unternehmens.
- Sie sagen wenig über die tatsächliche operative Effektivität der Controls aus.
- Die Qualität und Tiefe der Zertifizierungsaudits variieren stark.

Assurance- / Attestation-Reports

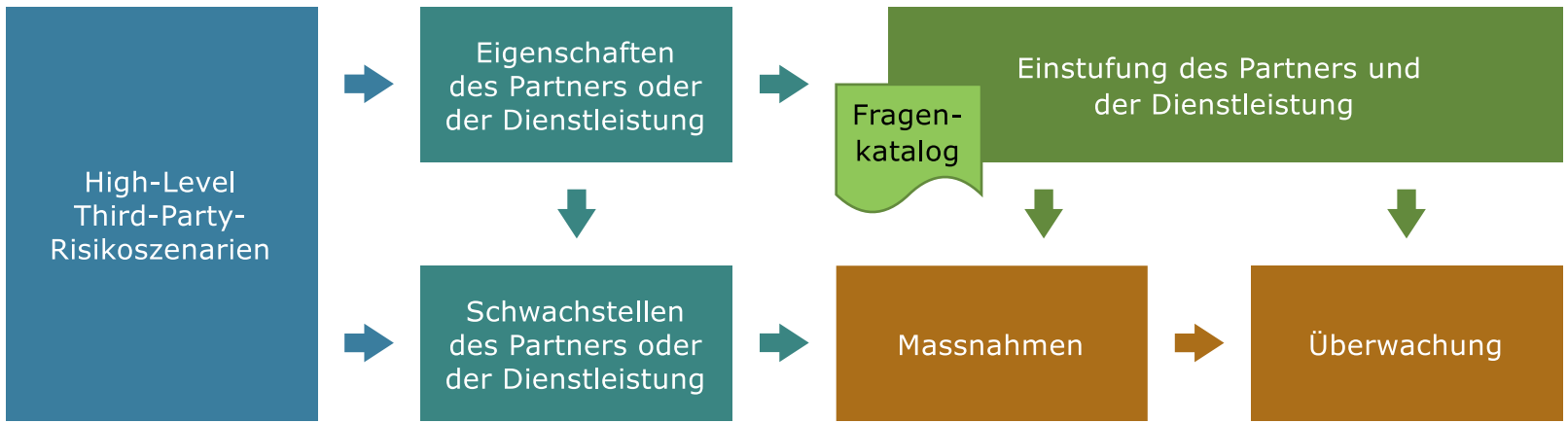
Grundlagen

- Eine unabhängige Prüfgesellschaft prüft die Kontrollen.
- Typischerweise nach ISAE 3000/3402 oder SOC1/SOC2
- Geprüft wird entweder nur der Aufbau (Type I) oder der Aufbau und die Wirksamkeit (Type II).

Auswahl der Kontrollen

- *Relevanz der Controls:* Der Kunde muss aktiv prüfen, ob die für sein Risikoszenario kritischen Kontrollen Teil der Prüfung waren.
- *Scoping:* Sind die richtigen Dienstleistungen und Standorte abgedeckt?
- *Inhalt vor Form:* Ein "sauberer" Bericht ohne relevante Prüfkriterien bietet keine echte Sicherheit.

TPRM-Framework



Vielen Dank.

Fragen?