Warth & Klein Grant Thornton

An instinct for growth™

eDiscovery

forensische Untersuchungen großer Datenmengen am Beispiel einer Sonderuntersuchung

Philipp Wiesauer – El Managero Diavolo
Sebastian Braun – El Consulterollo

Aachen, 18. Mai 2016

Vorstellung

Philipp Wiesauer

- Manager, M.Sc. Sichere Informationssysteme, ISO 27001 Lead Auditor
- Cybersecurity, IT-Forensic, eDiscovery, Data Analytics
- Durchführung und Leitung mehrerer Ermittlungsfälle in den Bereichen: Incident Response Investigation, Forensics, eDiscovery, Cybercrime, Data Leakage
- Über 3 Jahre Erfahrung bei KPMG, Forensic Technology
- Über 3 Jahre Erfahrung bei IBM

Warth & Klein Grant Thornton

An instinct for growth™

Vorstellung

Sebastian Braun

- Consultant, B.Sc. Angewandte Informatik
- Durchführung mehrerer Projekte in den Bereichen eDiscovery, IT-Forensic und Cybersecurity in unterschiedlichen Branchen (Industrie, Kanzlei, Beratung)
- Praxissemester und Bachelorarbeit beim LKA NRW

Warth & Klein Grant Thornton

An instinct for growth™

Agenda

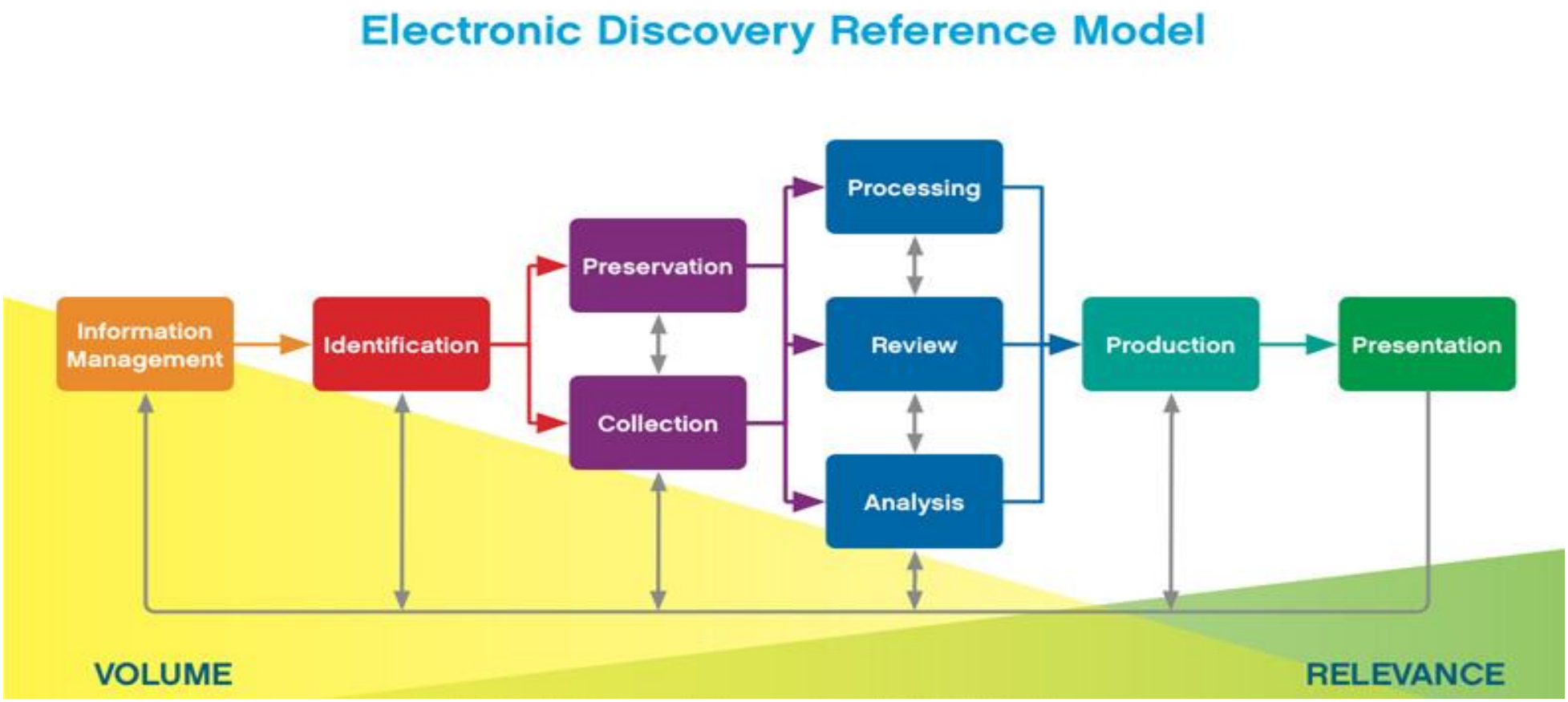
1. **Einleitung**
2. **Der eDiscovery Prozess - Überblick**
3. **Die Sonderuntersuchung**
4. **eDiscovery – die einzelnen Phasen**
   - DER – Digital Evidence Recovery
   - Vorverarbeitung
   - Data Processing
   - Review
5. **Resümee**

Warth & Klein Grant Thornton

An instinct for growth™

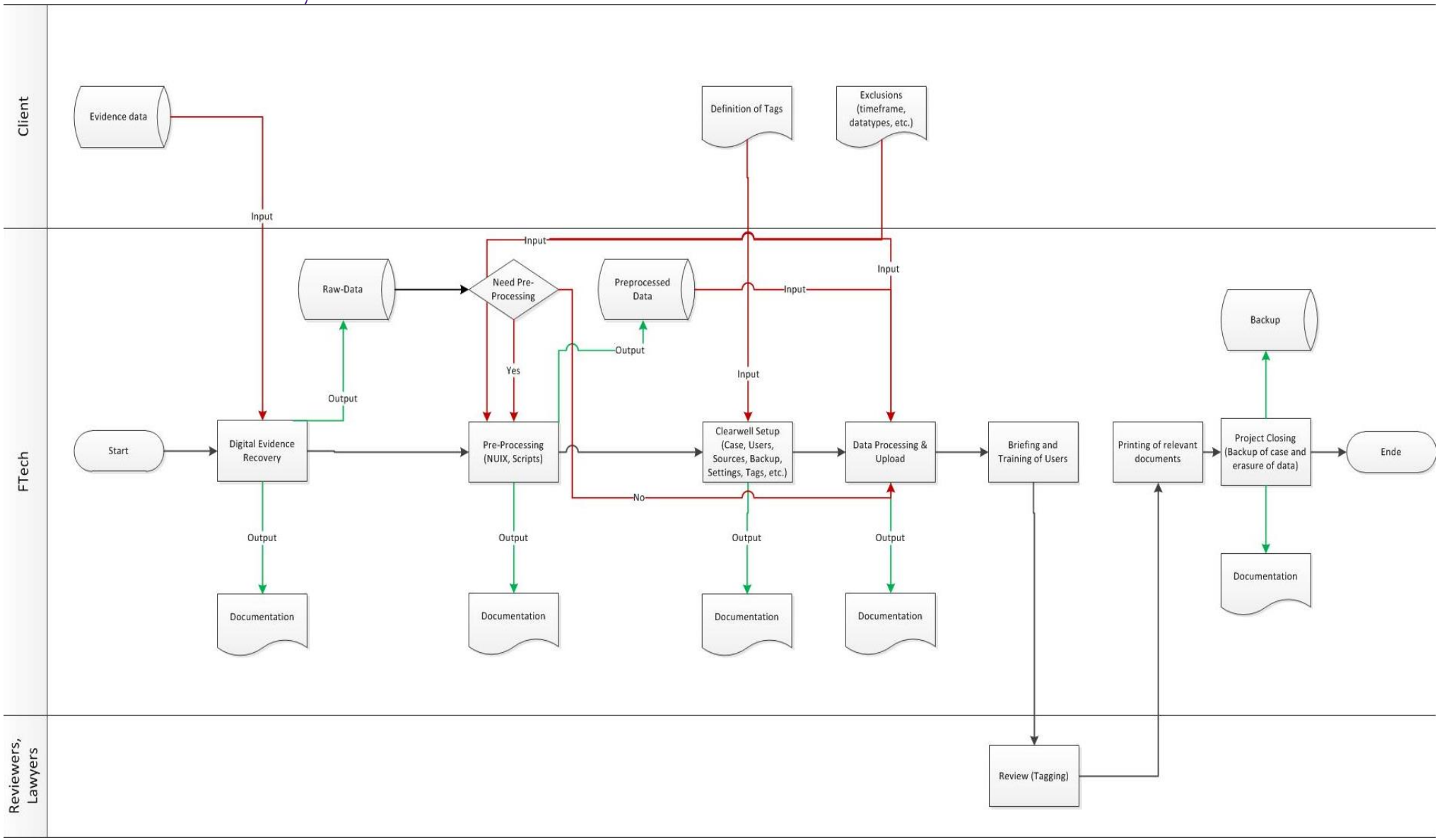
Der eDiscovery Prozess

eDiscovery Prozess



Quelle: www.edrm.net

eDiscovery Prozess



Sonderuntersuchung - Daten

- Finanzdienstleistungsbranche
- Über 100 Custodians
- Rohdaten ca. 15 TB
- Datenquellen: Homelaufwerke, Endgeräte, Mailpostfächer, Aktenordner …
  - Daten unterschiedlichster Typen
- Relevanter Betrachtungszeitraum: ca. 8 Jahre
- Verwendete Tools:
  - VERITAS Clearwell eDiscovery Platform
  - NUIX
  - X-Ways Forensics
  - Eigenentwicklungen

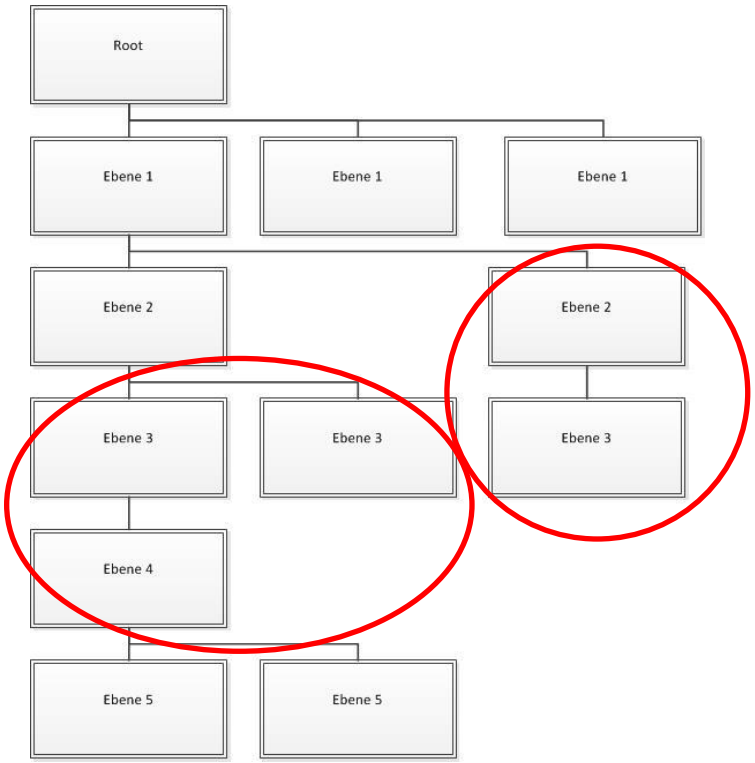
Die einzelnen Phasen des eDiscovery Prozesses

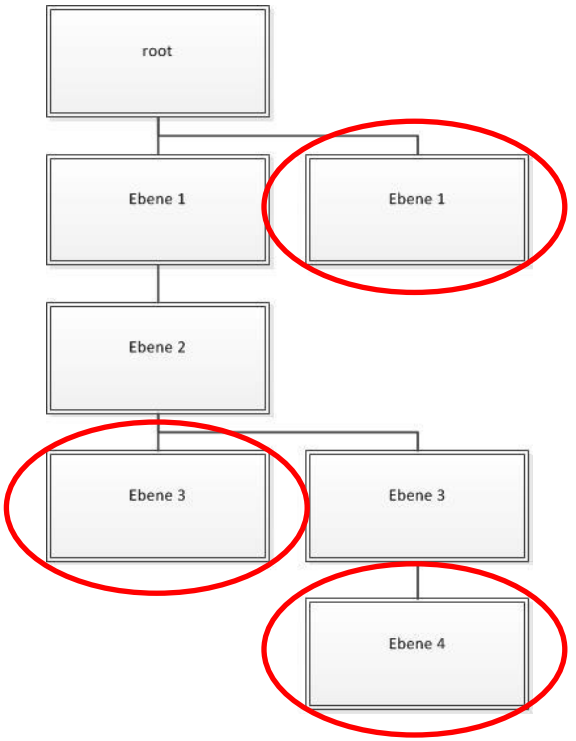
DER – Digital Evidence Recovery

- Forensisch korrekte Sicherung der Beweismittel
- Vorher zu klärende Problematik:
  - Datenschutz
  - Dürfen wir die Daten sichern?
  - Benötigen wir die Einwilligung der Custodians?
- Forensisch korrekt gesicherte Daten wurden vom Auftraggeber bereitgestellt
  - Dürfen wir diese Daten verarbeiten?
  - Datenschutzrechtliche Vorfilterung!

Vorverarbeitung (1/2)

- Sicherung von Systemen verschiedenster Strukturen
  - Skripbasierte Vorfilterung abgestimmt auf jedes einzelne System
- Beispiele:





Vorverarbeitung (2/2)

- NUIX (forensisches Tool)
  - Entpacken von Archiven
  - Herauslösen von Embeddings
  - Wiederherstellen gelöschter Daten
  - Deduplizierung
  - Identifikation korrupter Dateien
  - Filterung auf für Untersuchung relevante Dateitypen
  - Anwendung (sehr) umfangreicher und aufwendiger Suchwortlisten
  - Bereitstellen der Dateien zum Einspielen in die eDiscovery Plattform

Data Processing

- Clearwell (Veritas)
- Anlegen eines Cases:
  - Beweiskraft (Zeitzonen, Datums- und Zahlenformate…)
  - Concept Search
  - Predictive Coding
  - Stemming Search
- Nach Rücksprache mit dem Mandanten folgt nun die Erstellung des Tagsets
  - Wie viele verschiedene Kategorieebenen soll es geben?
  - Welche verschiedenen Kategorien werden benötigt?
  - Grundsätzlich: Tags für verschiedene technische Probleme

Data Processing

- Die durch Skripte und NUIX vorverarbeiteten Daten werden nun in die eDiscovery Plattform Clearwell eingespielt
- Clearwell Processing Optionen
  - Extrahierung aus Containern
  - Zu verarbeitende Dateitypen
  - Suchen unterschiedlicher Sprachen
- Fehlerbehebung!
  - Reparieren defekter E-Mail Postfächer
- Durch Vorverarbeitung und Deduplizierung konnte die relevante Datenmenge von 15 TB auf ca. 3 TB reduziert werden
- Strukturierung der eingespielten Daten zur effizienten Verteilung im Review

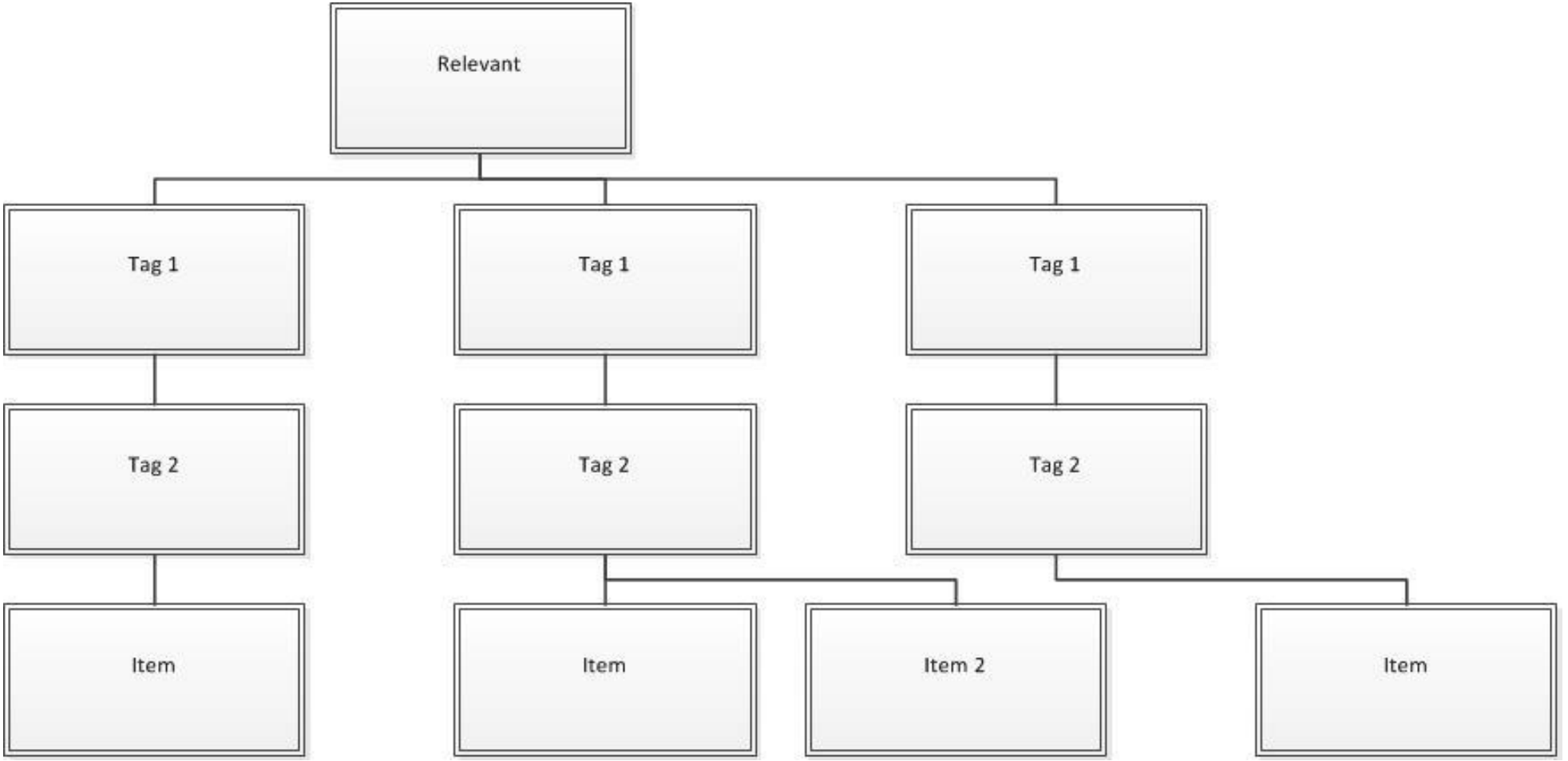
Review

- Im Review erfolgt die Durchsicht der in Clearwell eingespielten Dokumente
- Ein First Level Review zur groben Kategorisierung der Dokumente erfolgte durch Experten von WKGT
  - Briefing der Experten zur Thematik des Falles sowie zur Kategorisierung der Dokumente im First Level Review
  - Dauer: ca. 12 Monate
- Der weitere Review erfolgte durch die am Fall beteiligten Anwälte
  - Dauer: ca. 18 Monate

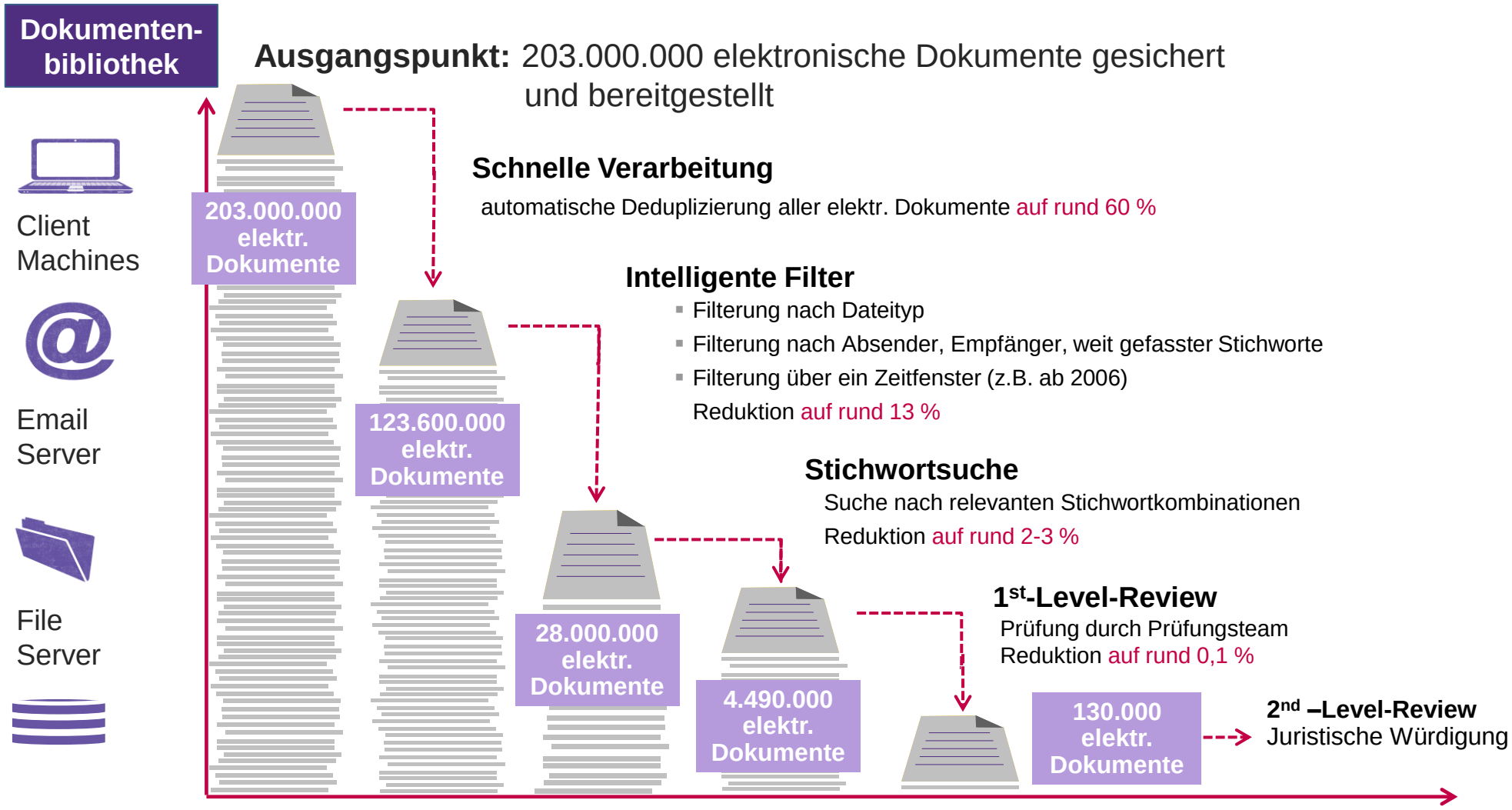
Bereitstellen von Dokumenten

- Zur Qualitätssicherung oder zur Auswertung durch die am Fall beteiligten Anwälte wurden in regelmäßigen Abständen Dokumentenanfragen gestellt
  - Die Dokumente sollten nach bestimmten Tagkombinationen in Ordner sortiert ausgeliefert werden
- Die entsprechenden Dokumente konnten mittels Suchspezifikation in Clearwell identifiziert und anschließend exportiert werden
- Zusätzlich wurden Metadateninformationen (vorhandene Tags pro Item etc.) aus Clearwell exportiert
- Mittels eigener Skripte wurden die Informationen aus den Metadaten mit dem Dokumentenexport abgeglichen und skriptbasiert die Form zur Bereitstellung hergestellt

Bereitstellen von Dokumenten



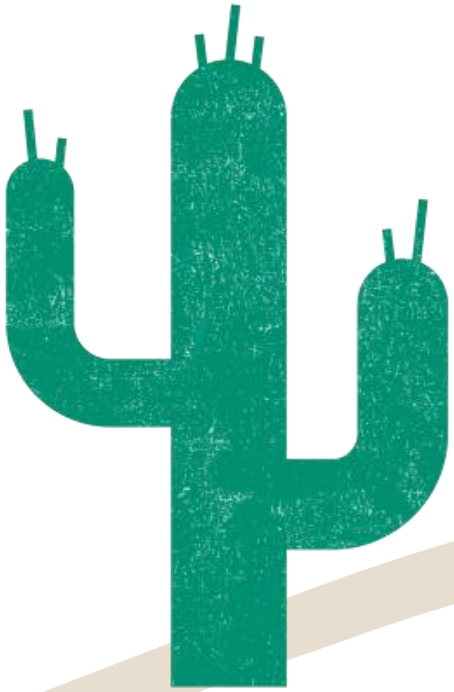
Resümee



Vielen Dank für Ihre Aufmerksamkeit

Warth & Klein Grant Thornton

An instinct for growth™



Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft

Warth & Klein Grant Thornton AG is a member of Grant Thornton International Ltd (Grant Thornton International).

The name Grant Thornton refers to Grant Thornton International or one of their member companies. Grant Thornton International and the member companies are no worldwide partnership. Each member provides it's service autonomously and independent from Grant Thornton International or other members.

wkgt.com