INFOTECH
[IT & Communication]

29. InfoTechDay

19.11.2024

HERZLICH WILLKOMMEN!

INFOTECH
[IT & Communication]

ISRM in der Praxis

Franz-Karl Schachinger, BSc.
Ing. Martin Mallinger, MSc.

Ihr Systemhaus.

INFOTECH
[IT & Communication]

Grundlagen

Information Security Risk Management Warum?

INFOTECH
[IT & Communication]

Normative Anforderungen
- ISO/IEC 27001
- ISO/IEC 27005
- ISO 31000
- COBIT
- NIST SP 800-30/39
- BSI IT Grundschutz
- IEC 62443-3-2:2020
- Etc.

Gesetzliche Anforderungen
- NIS-RL / NISG
- Wirtschaftsprüfung
- TKG
- Etc.

Best Practices
- CIS Controls (CIS RAM)
- OCTAVE
- FAIR
- Etc.

Vertragliche Anforderungen
- Je Organisation
- TISAX
- NIS2
  - Durch Kunden
  - An Lieferanten

Organisations-Entscheidungen
→ Risiken & Chancen

ISRM – Darum

INFOTECH
[IT & Communication]

ISRM =

Koordinierte Aktivitäten zur strategischen Lenkung und Steuerung einer Organisation

Minimierung möglicher Eintrittswahrscheinlichkeiten und Auswirkungen von Vorfällen

Transparente & methodische Entscheidungshilfe

Sicherstellung kontinuierlicher Geschäftsbetrieb durch behandelte Risiken

Maßnahmen-Priorisierung

Entwicklungstreiber

Eingliederung von ISRM

INFOTECH
[IT & Communication]

Informationsstand	Vorgehensweise	Methode
Nicht erkannte Risiken	Vorsorgen (Wahrscheinlichkeit & Auswirkung mindern)	Krisenmanagement (Business Continuity Management)
erkannte Risiken		**Risikomanagement**
bekannte Probleme	reaktiv beseitigen	Problemmanagement (Incident Management)

- **Information Security Risikomanagement**
  - Teil des Unternehmens-RM
  - Betrachtet IT- und Daten-Assets
  - Betrachtete Risiken betreffen:
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - (Authentizität)

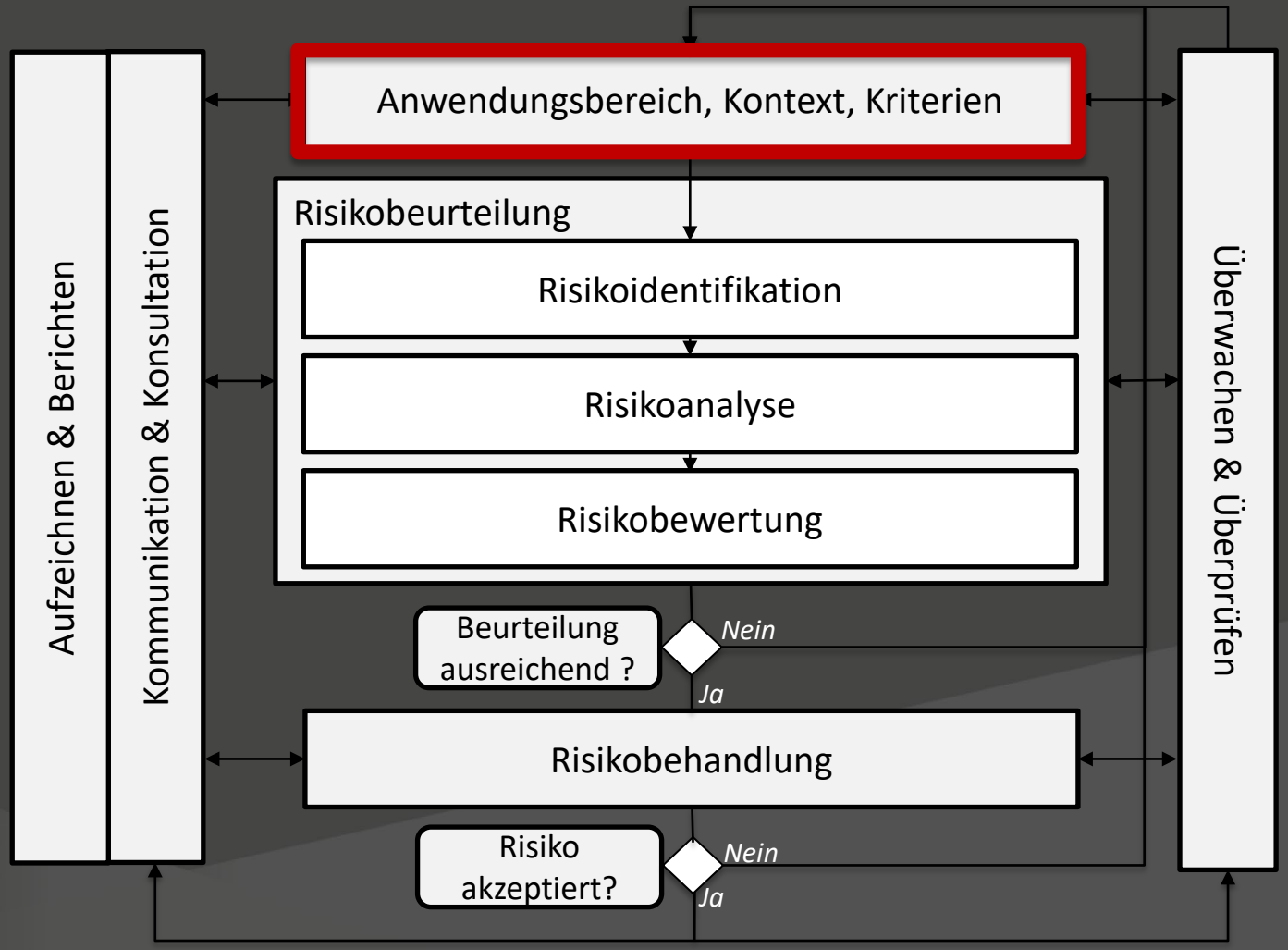
Allgemeine Definitionen

INFOTECH
[IT & Communication]

Risiko = Eintrittswahrscheinlichkeit * Schadensausmaß

- **Unterteilung Risiko in:**
  - Qualitatives Ergebnis: Hoch/Mittel/Niedrig
  - Quantitatives Ergebnis: monetäre Werte (€)

Prozess des Risikomanagements



1. Anwendungsbereich, Kontext, Kriterien

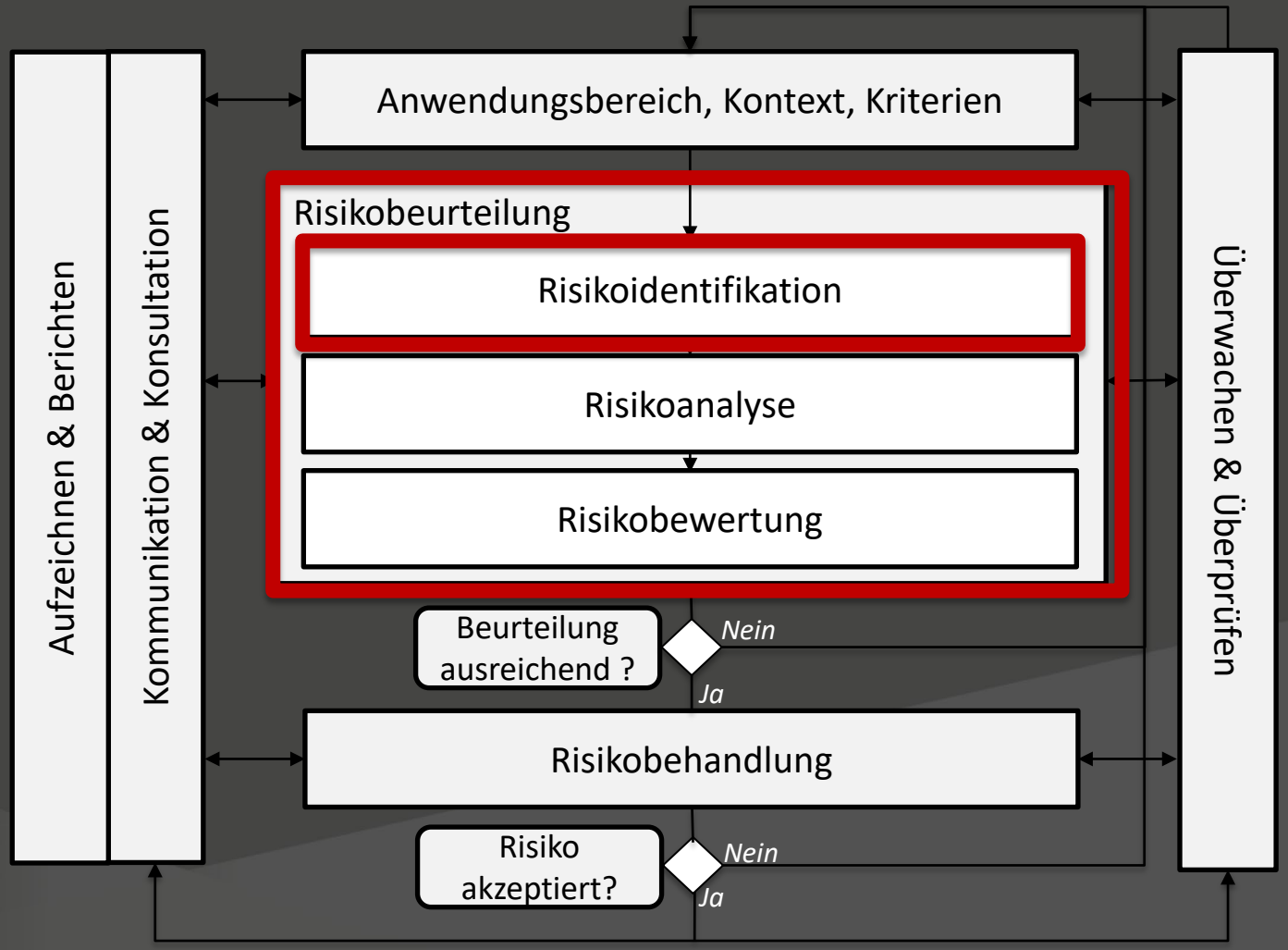
INFOTECH
[IT & Communication]

- **Evaluierung der kritischen Geschäftsprozesse**
  - Was Bedeutet ein Verlust der Vertraulichkeit/Integrität/Verfügbarkeit für den Prozess und das Unternehmen?

- **Für welchen Geschäftsprozess ist ein Risiko relevant?**

- **Identifikation von internen und externen Faktoren**

2. Risikobeurteilung



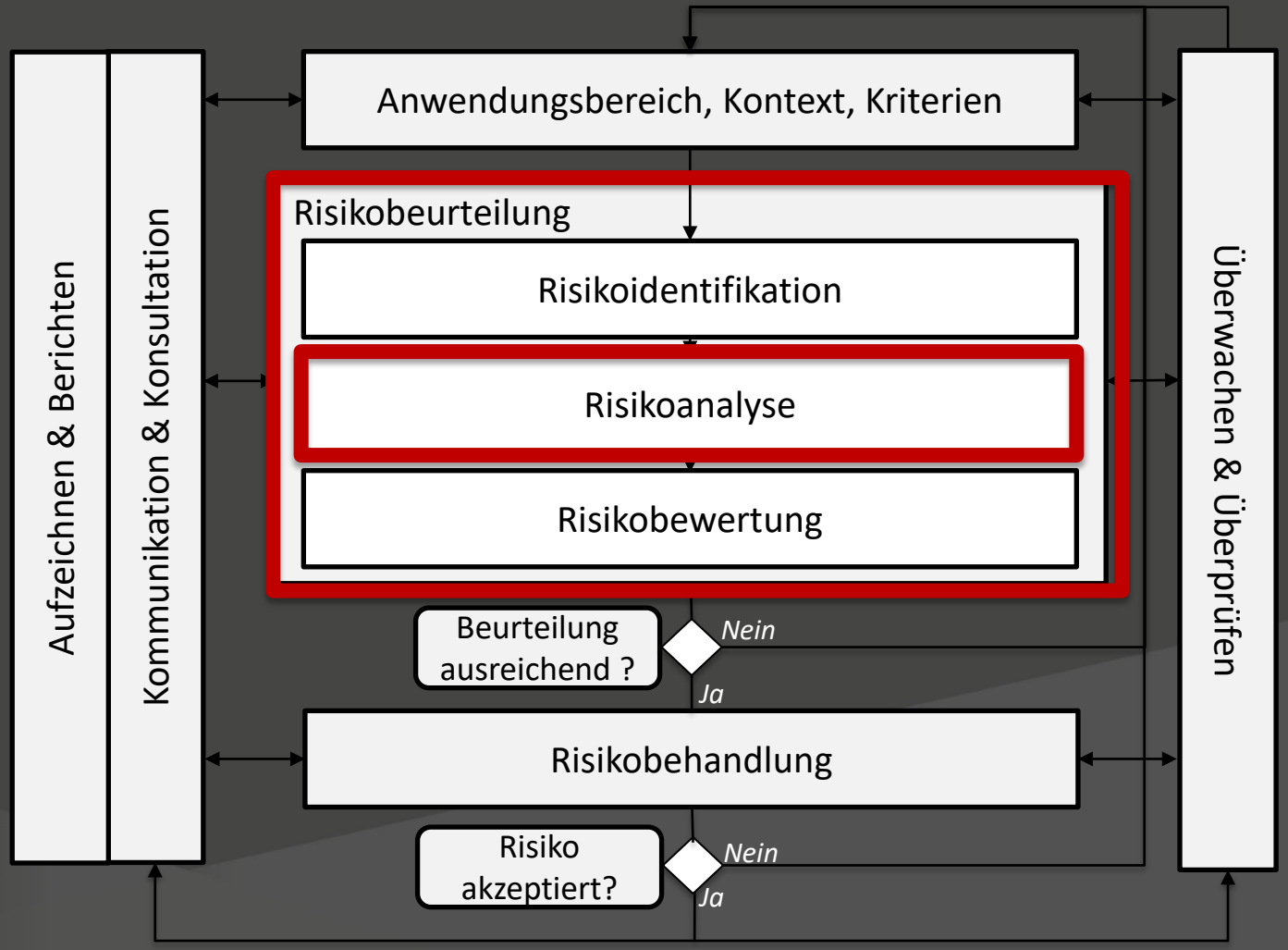
2. Risikobeurteilung

INFOTECH
[IT & Communication]

- **Welchem Risiko ist das Unternehmen durch eine konkrete Bedrohung ausgesetzt?**

1. **Identifikation:**
    - Nutzung unterschiedlicher Quellen und Kanäle (BSI, Audits, MITRE, News, ...)
    - **Was** ist davon betroffen?
    - Wer meldet das Risiko?
    - Welche Personen müssen eingebunden werden?
    - Status für Nachverfolgung festhalten
    - Zeitpunkt der Feststellung

2. Risikobeurteilung



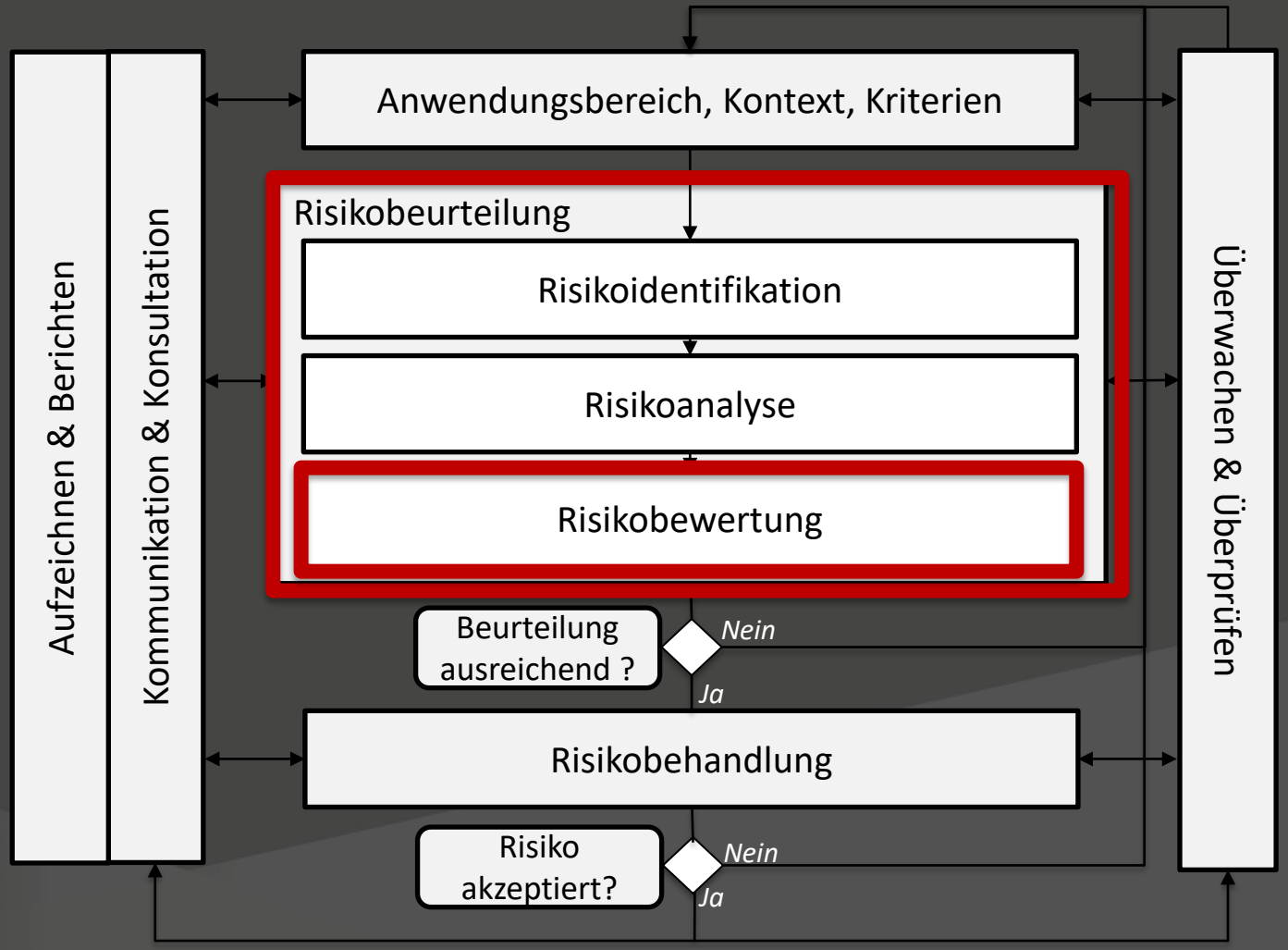
2. Risikobeurteilung

INFOTECH
[IT & Communication]

- **Welche Charakteristiken hat das Risiko?**

2. Analyse:
    - Wie hoch ist die **Entrittswahrscheinlichkeit**?
    - Die Art und Umfang der **Eintrittskonsequenzen**?
    - Komplexität und Zeitliche Faktoren
    - Gibt es bestehende Kontrollen/Maßnahmen und sind diese effektiv gegen das Risiko?

2. Risikobeurteilung



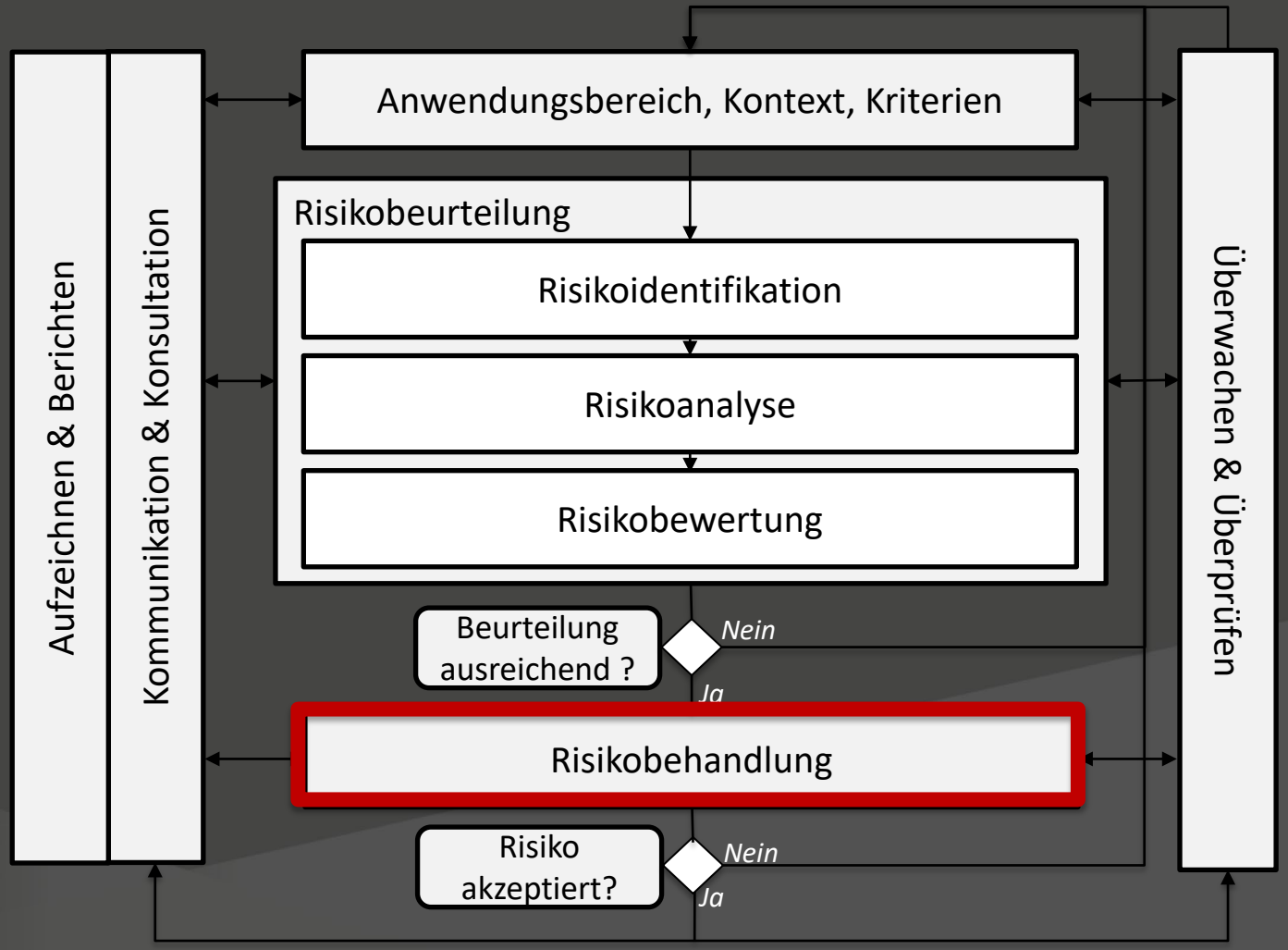
2. Risikobeurteilung

INFOTECH
[IT & Communication]

- Die Risikobewertung ist Entscheidungsbasis ob und welche weiteren Maßnahmen notwendig sind.

3. Bewertung:
    - Klassifizierung des Risikos anhand:
      Risiko = Eintrittswahrscheinlichkeit * Schadensausmaß
    - Hoch / Mittel / Niedrig => Basis für Maßnahmen und Risikobehandlung sowie Priorisierung

3. Risikobehandlung

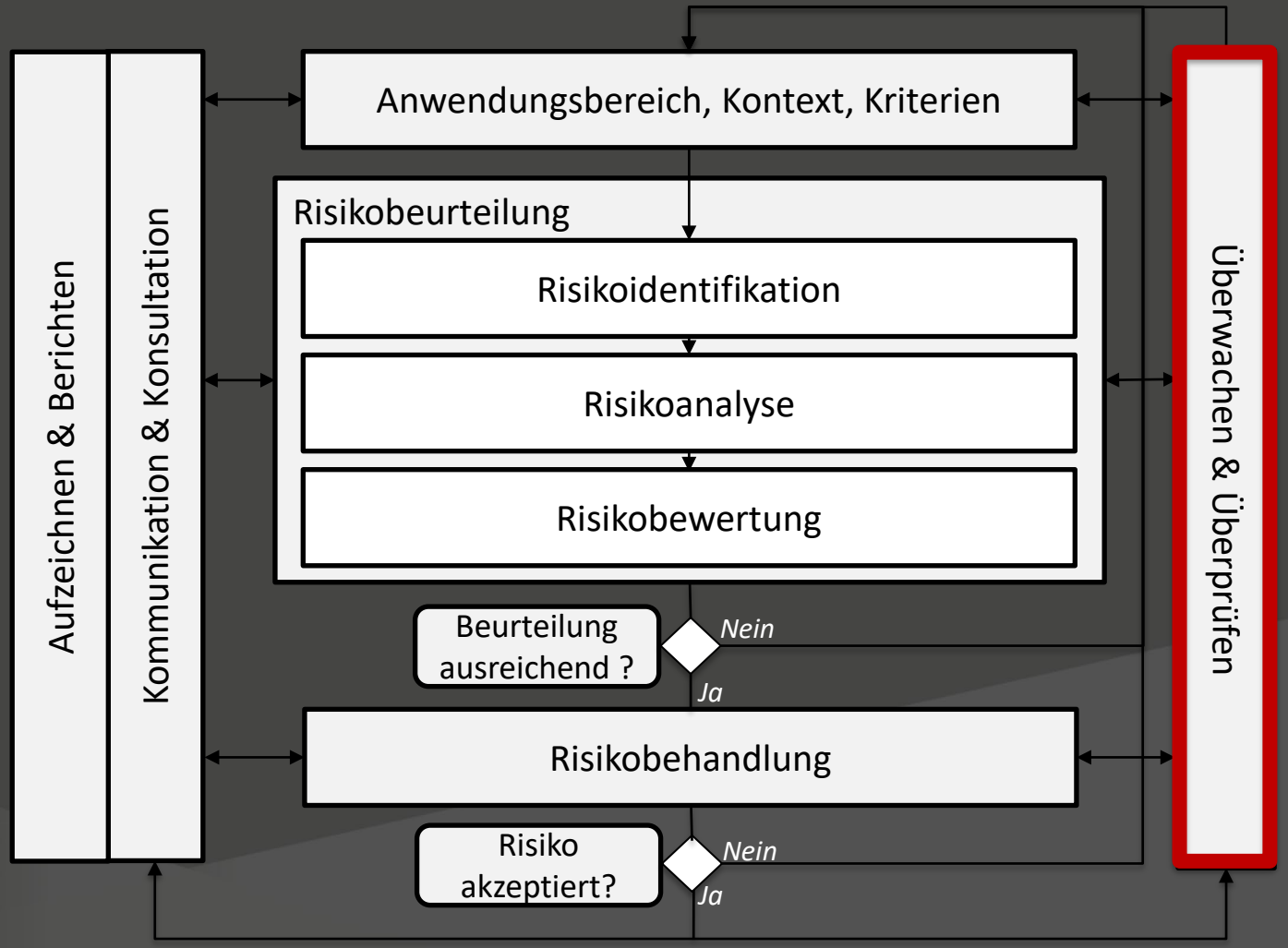


3. Risikobehandlung

INFOTECH
[IT & Communication]

- **Umsetzung von Maßnahmen, die das Risiko entfernen oder minimieren**
  - **Vermeiden:** Aktivität, die ein Risiko hervorruft wird eingestellt oder nicht gestartet
  - **Reduzieren**: Aktivitäten die entweder den Schaden oder die Eintrittswahrscheinlichkeit reduzieren
  - **Akzeptieren:** Risiko ist in akzeptablem Bereich für das Unternehmen
  - **Übertragen:** Abschluss Cyberversicherung, Verträge, Outsourcing der Risikobehafteten Dienste

Überwachen und Überprüfen



4. Risikoüberwachung

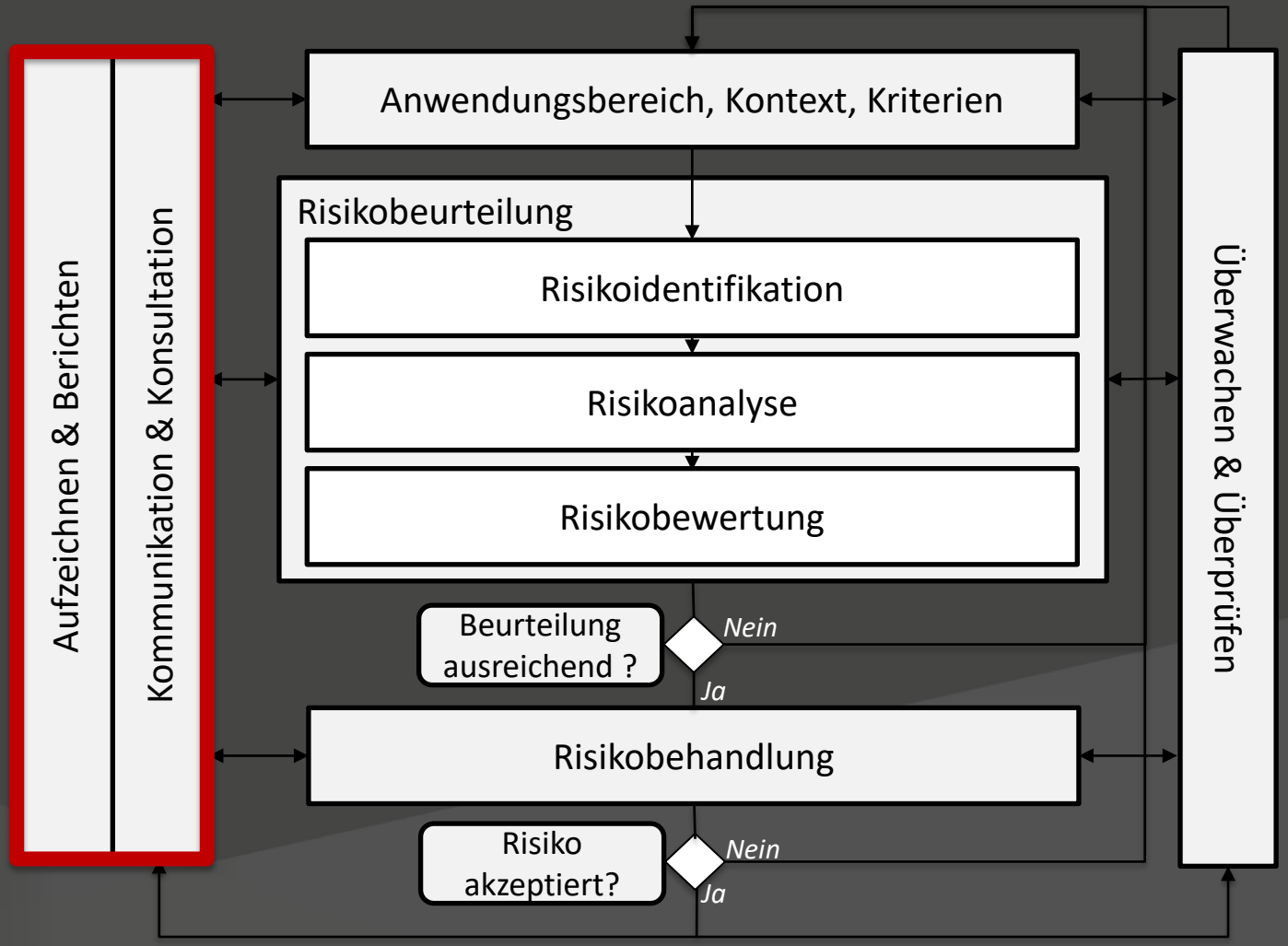
INFOTECH
[IT & Communication]

- Die Umsetzung der Behandlung muss bis zum Abschluss beobachtet werden.

- Auch nach Behandlung oder Akzeptanz des Risikos ist eine Fortwährende Beobachtung notwendig!
    - Gibt es ein verbleibendes Risiko nach der Behandlung?

- Informationssysteme und externe Einflüsse können sich rapide ändern und dementsprechend auch das Risiko.

Dokumentation und Kommunikation



5. Kommunikation und Dokumentation

INFOTECH
[IT & Communication]

- Regelmäßige Einbindung und Information der Stakeholder
  - Erhöht die Akzeptanz und Verständnis des ISRM
  - Integration des ISRM in Organisation
  - Engagement und Mitgestaltung validieren Ergebnisse

- Dokumentation von bewerteten Risken und der Prozess der Bewertung
  - Auch relevant für die Haftungsfrage im Schadensfall

INFOTECH
[IT & Communication]

Wie ?

Ihr Systemhaus.

Etablierung eines Risikomanagements

INFOTECH
[IT & Communication]

1. **Verstehen des Unternehmens und der Geschäftsprozesse**
    - Wie risikofreudig ist das Unternehmen? (Avers, indifferent, freudig)
    - Welche Wertschöpfungsprozesse werden durchgeführt?
    - Welche unterstützenden Prozesse gibt es?
    - Welche Kunden und Lieferantenbeziehungen gibt es ?
    - **Management Commitment für das Risikomanagementsystem**

2. **Erstellung und Zuweisung von Rollen, Verantwortlichkeiten und Befugnissen sowie Allokation von Ressourcen**
    - Meldender, Risk Owner,
    - Hierarchie, Umsetzung, Verfolgung, ...

3. Kommunikationswege und –tools sowie Dokumentationsmethoden
    - WER wird WIE über WAS informiert?
    - Welche Kommunikationsmittel werden verwendet (Vertraulichkeit)

Resümee

INFOTECH
[IT & Communication]

- **Es muss kein (teures) Tool verwendet werden**
  - Start mit Excel (keine Kosten / leicht anpassbar)
  - Grenze: Zusammenarbeit mit Einschränkungen
- **Es gibt keinen allgemeingültigen Universalprozess**
- **Es können auch Chance identifiziert werden**
  - sich vom Mitbewerber abzuheben,
  - Systeme zu optimieren,
  - Weiterentwicklung und Innovation zu fördern.
- **Transparenz / Absicherung**

INFOTECH

[IT & Communication]

Ihr Systemhaus.