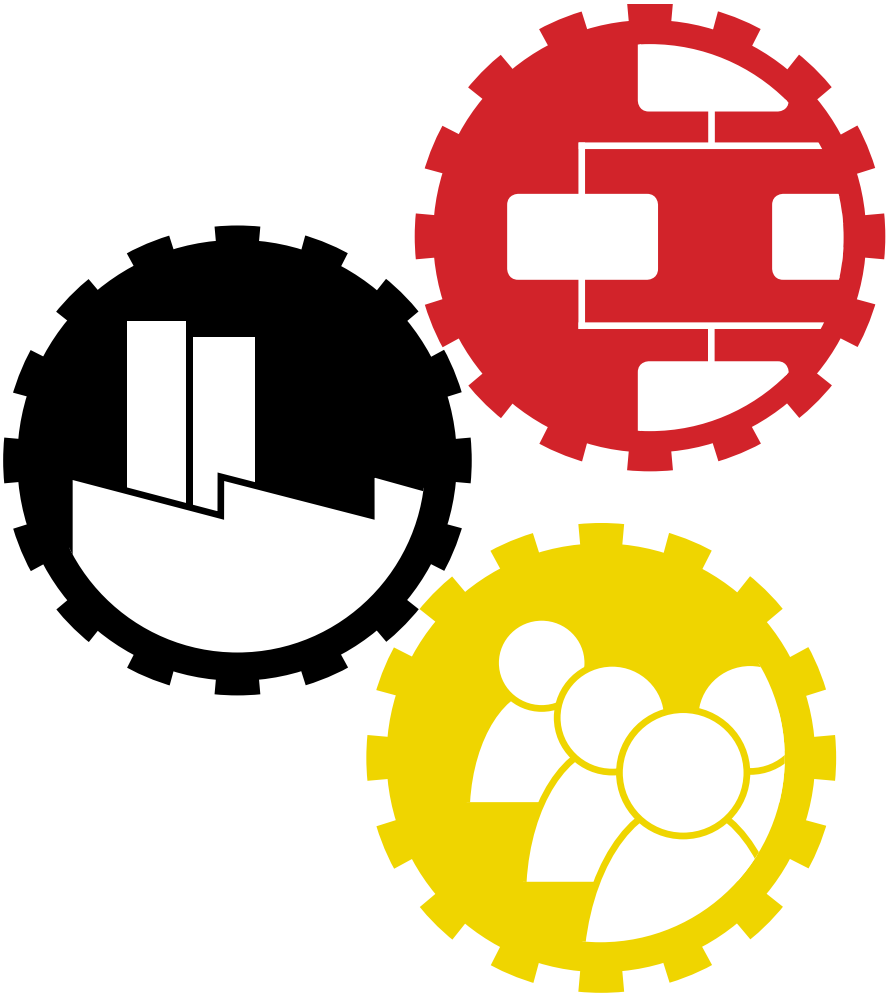
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

# Wirtschaftsgrundschutz

## Baustein ES1 Integritätsprüfung externer Parteien



# 1 Relevanzentscheidung für diesen Baustein

1. **Bribery Act**[1]: Operiert Ihre Institution im Vereinigten Königreich?
2. **Aktiengesellschaft**: Unterliegt Ihre Institution dem deutschen Aktiengesetz?
3. **Auslandsaktivitäten**: Handelt Ihre Institution gewerblich mit Gütern im Ausland?
4. **Finanzdienstleistungen**: Handelt es sich bei Ihrer Institution um ein Kreditinstitut, einen Finanzdienstleister, eine Versicherung oder eine Wirtschaftsprüfungsgesellschaft?
5. **Schlechte Erfahrungen**: Sind in der Vergangenheit Probleme mit Geschäftspartnern entstanden, die Sie durch sorgfältige Prüfung hätten vermeiden können?

Die fortschreitende Globalisierung führt dazu, dass viele Institutionen in neue Märkte und Regionen expandieren. Diese bergen nicht nur neue Chancen, sondern auch bisher unbekannte Risiken. Doch auch bereits erschlossene Märkte können risikoreich sein und sollten daher regelmäßig überprüft werden.

Haftungsrisiken

Bei Geschäftsanbahnungen oder Mergers & Acquisitions-Transaktionen wie Fusionen, Unternehmenskäufen oder Betriebsübergängen sollten die **Markt- und Geschäftsrisiken identifiziert werden**, um möglichen Fehlinvestitionen vorzubeugen. Für bestimmte Geschäfte schreiben nationale und internationale Normen wie der Foreign Corrupt Practices Act oder der UK Bribery Act die Durchführung von

[1] Die Der Bribery Act ist das Antikorruptionsgesetz des Vereinigten Königreichs. Die Besonderheit des Gesetzes ist, dass auch ausländische natürliche sowie juristische Personen sanktioniert werden können, die Verbindungen zu britischen Personen und Organisationen aufweisen.

Integritäts-Due-Diligence verpflichtend vor. Bei Nichteinhaltung der Gesetze sind die Institutionen, unter besonderen Voraussetzungen sogar die Leitung der Institution persönlich, für Schäden haftbar.

Mit Hilfe einer Integritätsprüfung externer Parteien (**Integritäts-Due-Diligence**) lassen sich so mit **geringem finanziellem Aufwand hohe Schäden vermeiden**. Letztendlich trägt sie zur Leistungsfähigkeit der Institution bei und sorgt dafür, dass mit Risiken kontrolliert umgegangen wird.

# 2 Beschreibung

Begriffsdefinition Integritäts-Due-Diligence

Der Begriff Integritäts-Due-Diligence (IDD) – auch bekannt als Third Party Due Diligence – bezeichnet die Einhaltung der Sorgfaltspflichten (engl. due diligence) durch die Überprüfung von Geschäftspartnern. Der Begriff wird jedoch auch synonym für die Durchführung einer **Überprüfung der Geschäftspartner** verwendet.

Gegenstand einer Integritätsprüfung

Durch die Durchführung einer IDD können Risiken bei Geschäftsaktivitäten mit einem neuen Geschäftspartner identifiziert und anschließend minimiert werden. Dabei spielt die Überprüfung folgender Faktoren eine entscheidende Rolle:

- Reputation des Geschäftspartners
- finanzielle Situation des Geschäftspartners
- wirtschaftliche Situation des Markts
- Verflechtungen mit Institutionen der gleichen Branche
- Authentizität des Geschäftspartners
- Hintergrund von Führungspersonen

**Ausschlaggebend** bei der IDD ist die Aufdeckung sogenannter **Warnsignale**. Darunter versteht man bestimmte Risikofaktoren, die darauf hindeuten, dass von der Erschließung des Markts bzw. der Geschäftsbeziehung abgesehen werden sollte, da anderenfalls erhebliche Risiken für die Institution drohen. Im Schadensfall können Haftungsansprüche gegenüber der Institution entstehen, da sie trotz der Warnsignale Geschäfte getätigt hat.

Warnsignale und Kriterien

Zu den Warnsignalen zählen u. a. die folgenden Kriterien:

- Mangel an Transparenz bezüglich des Managements und der Gesellschafterstruktur
- Unklarheit über die Vermögenswerte
- negative Reputation
- aktuelle Korruptionsvorwürfe
- Korruption in der Vergangenheit
- Verbindungen zum organisierten Verbrechen
- unangemessene politische Unterstützung
- Verdacht der Geldwäsche
- schlechte Leistungsbilanzen
- erhöhtes durchschnittliches Ausfallrisiko
- dubiose Firmenverflechtungen der Leitung der Institution
- Management oder Gesellschafter auf Negativlisten

Ziel der Integritätsprüfung

Ziel der IDD ist es, die **Integrität des Geschäftspartners zu verifizieren**. Auf diese Weise kann sichergestellt werden, dass die Geschäftsaktivitäten nach geltendem Recht und nach Vorgabe der Institutionsrichtlinien erfolgen. Des Weiteren werden **finanzielle Schäden präventiv abgewendet**.

# 3 Gefährdungslage

Geschäftsbeziehungen mit Partnern, die nicht nach geltendem Recht wirtschaften oder zu unseriösen Geschäften neigen, können drastische Auswirkungen auf eine Institution haben. Dazu zählen in erster Linie finanzielle Schäden, aber auch immaterielle Werte, wie bspw. die Reputation, können geschädigt werden. Darüber hinaus können Kosten durch Ermittlungs- und Gerichtsverfahren, Geldstrafen oder Sanktionen entstehen.

rechtliche Anforderungen

Eine sorgfältige **Prüfung der Geschäftspartner** ist daher oftmals erforderlich oder sogar gefordert. So schreiben der **Bribery Act 2010** (UK) sowie der **Foreign Corrupt Practices Act** (USA) die **Durchführung von IDD gesetzlich** vor. Dies betrifft nicht nur britische bzw. US-amerikanische Institutionen, sondern auch solche, die Verbindungen (Geschäftsverbindungen, Niederlassungen, Beteiligungen etc.) in Großbritannien bzw. den USA besitzen. Die Unterlassung der Überprüfung kann in beiden Ländern zu erheblichen Strafen führen. Doch auch in Deutschland sind IDDs empfehlenswert. Die Leitung einer Institution ist dazu verpflichtet, Sorgfalt bei der Geschäftsführung walten zu lassen (vgl. §§ 93, 116 AktG). Bei **Nicht-Einhaltung der Sorgfaltspflichten** können **Haftungsrisiken** entstehen. Die Durchführung einer IDD kann diese jedoch mindern.

Aus Geschäftsbeziehungen in unbekannten Märkten bzw. mit unbekannten Geschäftspartnern ergeben sich vielfältige Gefährdungen. Einige dieser Gefährdungen betreffen die Institution direkt und verursachen unmittelbare Schäden. Andere Gefährdungen wiederum

können auch indirekt oder verspätet eintreten. Dazu gehören bspw. Reputationsschäden.

Im Folgenden sind häufig auftretende Gefährdungen im Zusammenhang mit Geschäftsanbahnungen mit unbekannten Geschäftspartnern aufgeführt:

G 1 Bieterabsprachen
G 2 Korruption
G 3 Zahlungsunfähigkeit des Geschäftspartners
G 4 Industriespionage
G 5 Produktpiraterie
G 6 Politische Risiken
G 7 Scheinfirmen
G 8 Kriminelle Verflechtungen
G 9 Firmenverflechtungen/Interessenkonflikte
G 10 Verlust von Ansehen oder Vertrauen
G 11 Nichterbringung von Leistungen
G 12 Geldwäsche

# 4 Maßnahmen

Die **Prüfung der Integrität der Geschäftspartner** ist erforderlich, um einen **angemessenen Geschäftsbetrieb** sicherzustellen und **Schäden zu vermeiden**. Der Integritäts-Due-Diligence-Prozess stellt die hierfür zu implementierenden Verfahrensweisen und Methoden zur Konzeption, Umsetzung und Aufrechterhaltung bereit.

Die **Maßnahmen** folgen hierbei dem **Plan-Do-Check-Act-Regelkreis** und unterteilen sich in diese **drei wesentlichen Prozessblöcke**:

1. **Führungsprozess**
2. **Betriebsprozess**
3. **Berichts-/Kontrollwesen**

Abbildung 1 stellt dies grafisch dar.

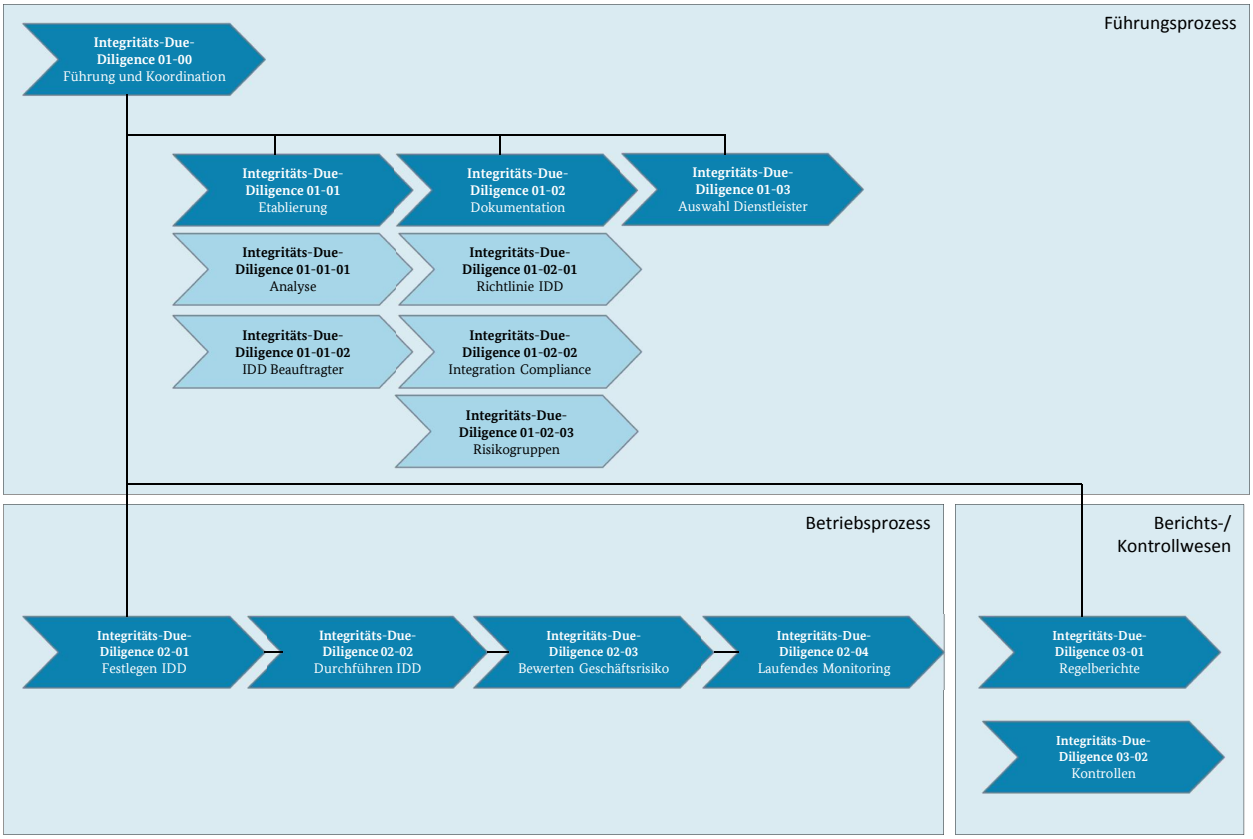



Abbildung 1: Prozessschaubild Integritäts-Due-Diligence

Die **Maßnahmen** dieses Bausteins sind **in drei Kategorien eingeteilt**. Sie richten sich nach dem **erforderlichen Detailgrad** bzw. der **gewünschten Ausprägung** (siehe Relevanzentscheidung) auf Basis der Anwendungsentscheidung gemäß Standard 2000-1:

**A-Kategorie – Basismaßnahmen**: unabdingbarer Wirtschaftsgrundschutz
**B-Kategorie – Standardmaßnahmen**: vollständiger Wirtschaftsgrundschutz
**C-Kategorie – erweiterte Maßnahmen**: erweiterter Schutz bei hohem Risikopotential

## *M 1 Entscheiden über die Durchführung einer IDD (A)*

Die **Entscheidung, ob** eine **IDD** von einer Institution **durchgeführt wird**, trägt die **Leitung der Institution**. Grundlage für diese Entscheidung können die eingangs erwähnten Gesetze sein, die IDDs zwingend erfordern.

relevante Gesetze

Dazu gehören vor allem die folgenden Gesetze:

- **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich** (KonTraG): Das KonTraG verpflichtet Vorstände und Aufsichtsräte von Unternehmen, ein **Früherkennungssystem für Risiken** einzuführen. Das KonTraG führte zur Ergänzung von § 91 AktG, wonach „der Vorstand geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (§ 91 (2) AktG). IDD wird dabei nicht explizit genannt, bildet aber eine „geeignete Maßnahme“ zur Erfüllung der Sorgfaltspflichten.
- **Aktiengesetz** (AktG): Das Aktiengesetz verpflichtet die Vorstands- und Aufsichtsrats¬mitglieder, die Geschäftsführung mit „Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“ (§§ 93 (2) und 116 AktG) zu übernehmen. Bei einem Schadensfall liegt die Beweislast beim jeweiligen Organ.
- **Geldwäschegesetz** (GwG): Im Gegensatz zum KonTraG und AktG wird das Geldwäschegesetz bei den Pflichten konkreter. Demnach müssen Kreditinstitute, Finanzdienstleister, Unternehmen und Personen, die E-Geld (digitales Geld) vertreiben, Finanz- und Versicherungsunternehmen, Rechtsanwälte, Wirtschaftsprüfer, Immobilienmakler, Spielbanken und Personen, die gewerblich mit Gütern handeln, ihre Vertragspartner identifizieren (§§ 2–3 GwG). Außerdem müssen Informationen zu Zweck und Art der Geschäftsbeziehung eingeholt werden. Der Vertragspartner muss weiterhin für einen wirtschaftlich Berechtigten handeln. Bei juristischen Personen besteht die Pflicht, die Eigentums- und Kontrollstruktur des Vertragspartners zu überprüfen. IDD deckt diese Maßnahmen ab und erfüllt somit die Sorgfaltspflichten.
- **Bribery Act 2010**: Gemäß dem britischen Bribery Act 2010 sind alle natürlichen und juristischen Personen mit Sitz in Großbritannien sowie ausländische Institutionen mit engen Verbindungen dorthin dazu verpflichtet, Präventionsmaßnahmen gegen Bestechung und Bestechlichkeit durchzuführen. Eine enge Verbindung können Mitarbeiter aus Großbritannien, eine Niederlassung oder geschäftliche

Beziehungen darstellen. Bei einem Bestechungsvorfall kann sowohl die Institution als auch deren Leitung belangt werden. Um Haftungsrisiken auszuschließen, legte das Ministry of Justice sechs Maßnahmen zur Bestechungsprävention vor. Dazu gehört u. a. die Durchführung von IDD.

- **Foreign Corrupt Practices Act** (FCPA): Der FCPA verpflichtet US-Unternehmen und US-amerikanische Privatpersonen und Beamte sowie ausländische Unternehmen, deren Wertpapiere an US-Börsen gehandelt werden, eine sogenannte FCPA Due Diligence durchzuführen. Dabei handelt es sich um eine IDD nach den Maßgaben des FCPA.

Neben gesetzlichen Grundlagen sprechen weitere Gründe für die Durchführung von IDDs. Dazu zählen insbesondere die **Minimierung wirtschaftlicher und finanzieller Risiken** bei M&A-Transaktionen, die **Reduzierung von Haftungsrisiken** bei Geschäftstätigkeiten sowie **negative Erfahrungen** hinsichtlich **der Integrität der Geschäftspartner** in der Vergangenheit.

### *M 2 Benennen eines IDD-Beauftragten (B)*

Aufgabe der Leitung

Die Institutionsleitung benennt einen **IDD-Verantwortlichen**. Dieser erarbeitet die Richtlinien, implementiert diese, führt die Untersuchungen durch, erstellt die dazugehörigen Berichte und entwickelt Empfehlungen für die Entscheidungsträger. Die **zu erfüllenden Sorgfaltspflichten** werden weder an den verantwortlichen Mitarbeiter noch an externe Dritte weitergegeben, sondern **verbleiben bei der Institutionsleitung**.

### *M 3 Aufnehmen von IDD in die Institutions-/Compliance-Richtlinien (A)*

Die Entscheidung über die Durchführung von IDD im Rahmen des Risikomanagements wird von der Institutionsleitung nicht nur getroffen, sondern auch getragen. Eine **ganzheitliche Implementierung der Maßnahmen** in den Wertekanon der Institution ist daher besonders bedeutsam für die effektive Umsetzung. Damit dies geschehen kann, wird **IDD in die Institutions- bzw. Compliance-Richtlinien**

**aufgenommen**, sodass ein verbindlicher Charakter entsteht. IDD wird dadurch zu einem Bestandteil der Compliance-Kultur der Institution.

### *M 4 Definieren von Risikogruppen (A)*

Sofern keine Gesetze die Durchführung einer IDD bei der Anbahnung von Geschäftsbeziehungen vorschreiben, ist es sinnvoll, **Risikogruppen** zu **definieren**. Diese klassifizieren institutionsintern Vertragspartner und beeinflussen somit, bei welchen Geschäftsaktivitäten und -partnern eine IDD durchgeführt werden muss. Außerdem kann je nach Risikogruppe der Umfang der IDD variieren. In der Regel wird ein mehrstufiges System angewandt. Jeder Risikogruppe werden dabei einzelne Maßnahmen zur Validierung der vorhandenen Informationen bzw. zur Risikoidentifizierung zugeordnet. Diese sind im Folgenden in den Maßnahmen M 7 bis M 14 zu finden.

Beispiele für risikoreiche Geschäftsbeziehungen

Besonders risikoreiche Geschäftsbeziehungen bestehen:

- in Ländern mit erhöhtem Korruptionsrisiko gemäß Korruptionswahrnehmungsindex
- bei Geschäftspartnern, die durch politisch exponierte Personen vertreten werden
- bei Transaktionen mit höheren Summen Bargeld
- bei Auftragsvermittlung durch Sales Agents oder Business Consultants
- bei institutionsspezifischen Risiken (bspw. Branchenzugehörigkeit)

Grundsätzlich gilt dabei, dass der **Geschäftspartner umso intensiver überprüft wird, je höher das Risiko des Geschäfts** ist.

### *M 5 Auswählen geeigneter Dienstleister (B)*

Je nach Größe und Struktur der Institution und ihrer **Geschäftsbeziehungen ist ein großer Personal- bzw. Zeitaufwand nötig, um** die **IDD durchzuführen**. Daher können auch **externe Dienstleister** mit der Durchführung der IDD beauftragt werden.

Vor- und Nachteile externer Beauftragungen

Die **Durchführung** von IDDs **durch externe Dienstleister** hat den Vorteil, dass **Interessenkonflikten** innerhalb der Institution **vorgebeugt** und **Personal sowie andere Ressourcen gespart** werden. Dennoch birgt die Beauftragung eines Dienstleisters auch Risiken, weshalb bei der Auswahl besondere Sorgfalt geboten ist. Die Auswahl des Dienstleisters erfolgt unter Berücksichtigung konkreter Qualitätsanforderungen. Dazu gehören die **Datenschutzkonformität** (national sowie international) und ein **funktionierendes Qualitätsmanagement**. Dies ist im besten Fall von einer unabhängigen Stelle gemäß ISO 9001 zertifiziert. Besonders bei Überprüfungen im Ausland setzen Dienstleister auch Partner für Recherchen vor Ort ein. Diese sollten vom Dienstleister ebenfalls regelmäßig geprüft werden.

Datenhaltung

Personenbezogene Daten sind stets **sensible Daten**, die **besonders schutzbedürftig** sind. Deshalb sollte bei der Dienstleisterwahl auch beachtet werden, dass die **gespeicherten Daten in Deutschland oder in Ländern mit vergleichbarem Datenschutzniveau verbleiben, um das Risiko von Datendiebstahl oder anderweitigem Verlust (z. B. durch behördliche Beschlagnahme) zu minimieren**.

### *M 6 Beschreiben der Anforderungen an die IDD (A)*

Jede Institution legt individuelle Anforderungen an die IDD fest. Diese richten sich nach Art und Zweck der Geschäftsbeziehungen sowie nach deren potentiellen Risiken. Somit erhält jede Risikogruppe unterschiedliche Anforderungen. Diese bauen regelmäßig aufeinander auf.

Die Anforderungen beschreiben, welche Maßnahmen durchgeführt werden, um die Integrität des Geschäftspartners zu überprüfen. Dabei kann zwischen **Erstmaßnahmen, Basismaßnahmen und erweiterten Maßnahmen** unterschieden werden. Welche Maßnahmen im konkreten Fall durchgeführt werden, richtet sich nach der eingestuften Risikogruppe. Im Allgemeinen ist der Umfang der IDD bei risikoreichen Geschäften größer als bei risikoarmen Aktivitäten.

Einzelne Maßnahmen zur Durchführung von IDD werden im Folgenden beschrieben.

### *M 7 Abgleichen mit Negativlisten (A)*

**Negativlisten** führen juristische und natürliche Personen auf, die erhöhte Korruptionsrisiken aufweisen oder mit denen **keine Geschäfte getätigt werden dürfen**. Diese Listen werden von verschiedenen Institutionen auf nationaler und internationaler Ebene veröffentlicht und regelmäßig aktualisiert. Da es weltweit über 1300 relevante Listen gibt, empfiehlt sich der Rückgriff auf spezielle Datenbanken, die diese Listen regelmäßig aktualisieren. Kostenpflichtige Anbieter solcher Datenbanken sind bspw. Dow Jones oder LexisNexis.

Zu diesen Listen gehören insbesondere:

Beispiele für Negativlisten

- Korruptionslisten
- Sanktionslisten
- Terroristenlisten
- Watch-Listen
- Embargo-Listen
- PEP-Listen (politisch exponierte Personen)

Ein **Abgleich** des Geschäftspartners mit den genannten Listen **ist nicht zeitintensiv** und stellt **dennoch** ein recht **effektives Mittel des Risikomanagements** dar. Kriminelle Geschäftspartner sowie risikoreiche Personen und Institutionen werden so schnell identifiziert.

### *M 8 Verifizieren von Basisinformationen (A)*

Die Verifizierung von Basisinformationen gibt eine grundlegende Auskunft über die Identität des Geschäftspartners. Die Verifizierung beinhaltet Basisinformationen wie die **Kommunikations- und Registrierungsdaten**, den **Geschäftszweck, Informationen zur Leitung** und zum **Schlüsselpersonal** des Geschäftspartners sowie zur **Historie**. Durch diese Maßnahme wird jedoch nicht sichergestellt, dass der Geschäftspartner seriös wirtschaftet. Vielmehr bietet sie nur die Bestätigung, dass der Partner offiziell registriert ist und über eine ordentliche Struktur verfügt.

### *M 9 Überprüfen der finanziellen Informationen (B)*

Um Zahlungsverzögerungen und -ausfälle des Geschäftspartners im Vorfeld zu vermeiden, ist eine **Überprüfung** seiner **finanziellen Situation äußerst empfehlenswert**. Viele Institutionen sind gesetzlich dazu verpflichtet, Bilanzen und Jahresabschlüsse zu veröffentlichen oder tun dies – im Rahmen ihres Compliance-Programms – freiwillig.

Darüber hinaus können Informationen von Kreditratingagenturen oder Auskunfteien hinzugezogen werden. Diese geben oftmals Aufschluss über die **Bonität des Geschäftspartners**.

Neben der Überprüfung aktueller Finanzinformationen sollte auch die finanzielle Vergangenheit des Geschäftspartners analysiert werden. Insolvenzen, Zahlungsschwierigkeiten und andere negative Indikatoren werden dadurch entdeckt.

### *M 10 Analysieren von Firmenbeteiligungen (B)*

Korruptionsrisiken

Geschäftspartner – sowohl juristische als auch natürliche Personen –, die enge Verbindungen zu Institutionen der gleichen Branche besitzen, weisen ein erhöhtes Risiko von Korruption und Vetternwirtschaft auf. Daher werden Art und Zweck von **Firmenverflechtungen** der zu überprüfenden Institution sowie ihr **Schlüsselpersonal** besonders genau **untersucht**. Mithilfe von lokalen Dienstleistern, offiziellen Melderegistern und Auskunfteien werden Firmenbeteiligungen einzelner Personen und Institutionen identifiziert. Eine Analyse der Verbindungen kann bestimmte **Warnsignale** wie auffällige Geschäfte aufdecken.

Analysekriterien für Firmenbeteiligungen

Bei der Analyse von Firmenbeteiligungen werden folgende Kriterien betrachtet:

- Funktionen als Gesellschafter
- Positionen in Kontrollgremien
- Positionen im höheren Management
- sonstige Positionen und Funktionen
- Tochtergesellschaften
- Mutterkonzerne

### *M 11 Recherchieren in verschiedenen Medien (C)*

Durch die **Recherche in Presseberichten** und anderen **öffentlichen Publikationen** kann ein **Überblick über** die **Reputation** des potentiellen Vertragspartners gewonnen werden. Vor allem das Internet bietet eine Vielzahl von Möglichkeiten, Erfahrungen anderer Personen oder Institutionen mit dem Geschäftspartner festzustellen. Auch Skandale oder Verdachtsfälle im Zusammenhang mit dem Geschäftspartner können auf diese Weise in Erfahrung gebracht werden.

Bei der Suche können verschiedene Quellen genutzt werden. Dazu zählen insbesondere:

Quellen

- Suchmaschinen
- Fachpublikationen
- Mediendatenbanken
- Archive

Die Wahl der Instrumente und die Tiefe der Suche richten sich nach der **Relevanz der Geschäftsbeziehung, der Risikogruppe** und **möglicherweise gefundenen Auffälligkeiten**.

### *M 12 Verifizieren der Geschäftsadresse (C)*

Die Verifizierung der Basisinformationen in offiziellen Registern bietet lediglich ein Indiz für die Authentizität der Angaben. Um sicherzustellen, dass der Geschäftspartner tatsächlich operativ tätig ist, sollte die **Geschäftsadresse verifiziert** werden. Dazu wird **vor Ort geprüft, ob** der **potentielle Partner** an der Adresse **lokalisiert werden kann** (bspw. anhand von Hinweistafeln, Briefkästen etc.) und ob ggf. plausible **Geschäftsaktivitäten erkennbar sind**. Zur Beweissicherung wird eine Fotodokumentation, auch **Local Check** genannt, angefertigt. Dabei werden alle Indizien dokumentiert, die für bzw. gegen Geschäftsaktivitäten sprechen.

### *M 13 Bewerten des Geschäftsrisikos (A)*

Auf Grundlage der gesammelten Daten über den Vertragspartner wird das **Geschäftsrisiko qualitativ ermittelt**. **Ziel** ist es, **risikoreiche**

**Geschäfte** zu **identifizieren und** einen **verlässlichen Vertragspartner** zu **finden**. Institutionen, bei denen es Warnsignale gibt, werden dabei grundsätzlich als risikoreiche Geschäftspartner angesehen. Geschäftsbeziehungen mit diesen Institutionen werden grundsätzlich vermieden, anderenfalls könnten finanzielle Verluste und Reputationsschäden entstehen. Ist eine Geschäftsbeziehung notwendig, werden **Maßnahmen zur Risikoreduzierung** getroffen, wodurch auch aus dem Geschäft resultierende Haftungsrisiken in der Regel minimiert werden.

## *M 14 Monitoren der Geschäftspartner (B)*

Nachdem neu akquirierte oder bestehende Geschäftsverbindungen sorgfältig überprüft wurden, werden diese einem **regelmäßigen Monitoring** unterzogen. Das Intervall hierfür richtet sich nach der Risikogruppe des Geschäfts, sodass risikoreiche Verbindungen regelmäßiger überwacht werden. Das Monitoring ist notwendig, da sich gerade im globalisierten Wirtschaftsmarkt Veränderungen sehr schnell einstellen können. Auch politische und wirtschaftliche Krisen können dazu führen, dass das Risiko einer Geschäftsbeziehung zu einem Partner steigt.

Überblick zu überwachender Risikofaktoren

Zu den Risikofaktoren, die fortlaufend oder in Intervallen überwacht werden, gehören bspw.:

- Kommunikationsdaten
- finanzielle Informationen
- Firmenverflechtungen
- Medienreputation
- Negativlisten

# 5 Weiterführende Informationen

Weiterführende Informationen zum Thema Integritäts-Due-Diligence können den nachfolgenden Veröffentlichungen[2] entnommen werden.

- *Mathias B. Welsch: Compliance Due Diligence: Minimierung von Haftungsrisiken beim Unternehmenskauf, Hamburg 2014*
- *United Nations Global Compact: 2B.IV Case Story: Integrity Due Diligence*
- *Ministry of Justice (UK): The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing, http://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf*

[2] Links zuletzt am 04.07.2017 auf Funktionalität geprüft.

# 6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

| Analyse | Organisation | Dokumentation |
|---|---|---|
| Erhebung des Bedarfs<br><br>Risikogruppen | IDD-Beauftragter<br><br>Auswahl geeigneter Dienstleister<br><br>Berichtswesen | Richtlinie zur IDD<br><br>Integration in bestehende Compliance-Regelwerke<br><br>Vorgehensweisen |

| Durchführung | Erkenntnisse |
|---|---|
| Verifizieren von Basisinformationen<br><br>Überprüfen der Finanzdaten und Beteiligungen<br><br>Verifizieren der Geschäftsadresse | Geschäftsrisiko<br><br>laufendes Monitoring |

Maßnahmenübersicht und -kategorien

| A - Basismaßnahmen | B - Standardmaßnahmen | C - erweiterte Maßnahmen |
|---|---|---|
| M 1 Entscheiden über die Durchführung einer IDD<br><br>M 3 Aufnehmen von IDD in die Institutions-/Compliance-Richtlinien<br><br>M 4 Definieren von Risikogruppen<br><br>M 6 Beschreiben der Anforderungen an die IDD<br><br>M 7 Abgleichen mit Negativlisten<br><br>M 8 Verifizieren von Basisinformationen<br><br>M 13 Bewerten des Geschäftsrisikos | A +<br><br>M 2 Benennen eines IDD-Beauftragten<br><br>M 5 Auswählen geeigneter Dienstleister<br><br>M 9 Überprüfen der finanziellen Informationen<br><br>M 10 Analysieren von Firmenbeteiligungen<br><br>M 14 Monitoren der Geschäftspartner | A und B +<br><br>M 11 Recherchieren in verschiedenen Medien<br><br>M 12 Verifizieren der Geschäftsadresse |

# Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Bausteins einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgenden Autoren und Mitwirkenden: Herr Martin Koos, Herr André Schwietzke, Herr Eckhard Neumann (SIGNUM Consulting GmbH).

# Impressum

**Herausgeber**
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

**Herausgeber**
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

**Herausgeber**
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

**Redaktion/Bezugsquelle/Ansprechpartner**
Prof. Timo Kob (Gesamtprojektleitung)

**Gestaltung, Produktion**
HiSolutions AG

**Stand**
Juli 2017

**Auflage**
1. Auflage