IT-Governance, Risiko und Compliance

Alfabet-Referenzhandbuch

Dokumentationsversion Alfabet 10.13.1

Konventionen für die Dokumentation

Konvention	Bedeutung
Fett	Wird für alle Elemente verwendet, die auf der Benutzeroberfläche dargestellt werden, wie zum Beispiel Menüelemente, Schaltflächen, Registerkarten, Dialogfelder, Titel von Ansichtsseiten und Kommandos. Beispiel: Klicken Sie nach Beenden des Setups auf **Fertigstellen**.
Kursiv	Wird für Hervorhebungen und Verweise auf Dokumententitel und Kapitel-überschriften verwendet. Wird im Code für Variablen verwendet Beispiel: Informationen hierzu finden Sie im Referenzhandbuch *Administration*. Beispiel: `<XmlElement XmlAttribute="Anwendername"/>`
Anführungszeichen oben	Kennzeichnet einzugebende Werte und feststehende Namen im Text. Beispiel: Wenn der Objektstatus “Aktiv” ist, dann...
Begriffe komplett in Großbuchstaben	Tastaturtasten Beispiel: STRG+UMSCHALT
Datei > Öffnen	Wird für Menüaktionen verwendet, die vom Anwender durchzuführen sind. Beispiel: Um die Applikation zu schließen, wählen Sie **Datei** > **Beenden**
< >	Steht für Variablen, die vom Anwender eingegeben werden. Beispiel: Erzeugen Sie einen neuen Anwender und geben Sie <Anwendername> ein. (Ersetzen Sie den Begriff inklusive Klammern mit dem jeweiligen aktuellen Wert.)
	Dies ist ein Hinweis, der Zusatzinformationen gibt.
	Dies ist ein Hinweis, der Prozessinformationen gibt.
	Dies ist ein Beispiel.
	Dies ist eine Warnung.

Inhaltsverzeichnis

Kapitel 1: Einführung in IT-Governance, Risiko und Compliance 5

Kapitel 2: Applikationsrisikomanagement 8

Methodik: Risikomanagement verstehen 9

Voraussetzungen: Konfigurationsanforderungen für das Risikomanagement 11

Verständnis der Governance und Zuständigkeiten im Applikationsrisikomanagement 12

Erfassung von Bedrohungen und Definition von Risikominderungsvorlagen 12

Definition von Bedrohungsgruppen und Erfassung von Bedrohungen 13

Angeben von Risikominderungsvorlagen für den Bedrohungskatalog 14

Verstehen der Applikationsrisiken basierend auf vorhandenen Bedrohungen 15

Bewerten von Objekten für Risikorelevanz 15

Erzeugen von Risikomanagementgruppen 17

Bewertung der Relevanz von Objekten für die Risikobewertung 18

Durchführung der Risikobewertung von Applikationen 19

Bewertung von Applikationen für Risiken 20

Analysieren der Risikobewertung 21

Erfassen und Verwalten von Risikominderungen 21

Verwalten und Speichern der Daten über die Risikobewertung 22

Kapitel 3: Informationsrisikomanagement 23

Kapitel 4: Projektrisikomanagement 25

Kapitel 5: Compliance-Management 26

Methodik: Verstehen des Compliance-Managements 27

Voraussetzungen für Compliance-Management 30

Festlegen von Compliance-Katalogen und Compliance-Domänen 31

Initiieren und Verwalten von Compliance-Projekten 34

Bewerten der Zielobjekte des Compliance-Projekts 37

Kapitel 1: Einführung in IT-Governance, Risiko und Compliance

Unternehmen müssen IT-Strategien, Architekturen und Prozesse effektiv bewerten, planen und verwalten, indem sie mögliche Schwachstellen, Bedrohungen und Risiken für ihre IT verstehen. Die Bewertung von Bedrohungen sowie die Einhaltung verschiedener Anforderungen sind auf jeder Planungsebene notwendig, um Risiken für die IT-Umgebung Ihres Unternehmens zu reduzieren. IT-Risikomanagement sollte kein einmaliges Projekt sein, sondern ein kontinuierlicher Prozess, der auf sich ständig verändernde IT-Risiken und Geschäftsumgebungen abzielt und sicherstellt, dass die Risiken kontinuierlich überwacht und die Risikomanagementstrategie entsprechend angepasst wird.

Mit dem Vertriebspaket „IT Governance, Risk and Compliance“ können Sie die Anforderungen Ihres Unternehmens in Bezug auf das Verständnis und die Minimierung von Risiken sowie die Erfüllung von Compliance-Anforderungen realisieren. Die Ermittlung der richtigen Richtlinien für IT-Risiken, Compliance und Sicherheit ist ein Balanceakt zwischen dem Bedürfnis des Unternehmens nach Agilität und Kontinuität und der Forderung nach Einhaltung von Vorschriften. Die im Vertriebspaket „IT Governance, Risk and Compliance“ verfügbaren Funktionen ermöglichen es Ihnen, die aktuellsten und relevantesten IT-Schwachstellen im Unternehmen zu verstehen und die erforderlichen Maßnahmen zu planen und zu überwachen, um die Auswirkungen der von ihnen ausgehenden Risiken zu minimieren und die Kosten und den Aufwand für die Bewertung und das Management von Compliance und Risiken auszugleichen.

Das Paket "IT Governance, Risk and Compliance" wird von Unternehmensarchitekten, Compliance-Verantwortlichen, Risikomanagern und Wirtschaftsprüfern für folgende Zwecke eingesetzt:

- Bewertung von Applikationen, Daten und Projekten und anderen (IT)-Objekten entsprechend ihrem Gefährdungspotenzial
- Festlegung von Bedrohungs-, Risiko- und Risikominderungskatalogen, die auf bestimmte Applikationen, Technologien, Projekte usw. anwendbar sind.
- Automatisierung der Bewertung von Bedrohungen und Risiken und deren Minderung
- Etablierung automatisierter Prozesse zur Durchführung von Risikobewertungen auf der Grundlage sich ständig weiterentwickelnder Bedrohungen auf dem Markt
- Verfeinerung der Richtlinien zur Datenaufbewahrung auf einer detaillierteren Ebene
- Durchführung und Verwaltung von Compliance-Bewertungen
- Definition eines zentralen Frameworks, um die Compliance-Prüfung effizienter zu gestalten
- Prüfung auf Einhaltung der Kontrollstruktur und Richtigkeit der bewerteten Objekte

Um die potenziellen Schwachstellen in der IT zu verstehen und Projekte zu deren Behebung zu implementieren, bietet Alfabet Risikomanagement und Compliance-Management sowie die Durchführung von konfigurierbaren Befragungen zur Initiierung komplexer Datenerfassungsaufgaben an. Die Risikomanagement-Funktionalitäten in Alfabet unterstützen die Risikobewertung, die es ermöglicht, Objekte wie Applikationen, Geschäfte, Daten, Projekte usw. im Unternehmen im Hinblick auf ihr Risiko zu bewerten und Maßnahmen zur Verhinderung oder Reduzierung der Risiken zu definieren und zu planen. Die in Alfabet verfügbaren Risikomanagement-Funktionalitäten können für die Funktionen Applikationsrisikomanagement, Informationsrisikomanagement und Projektrisikomanagement implementiert werden. Bewertungen können mit Workflows automatisiert werden, was den manuellen Aufwand drastisch reduziert. Darüber hinaus können Sie die erforderlichen IT-Kontrollen definieren, um Risiken zu minimieren und gesetzliche und unternehmensinterne Compliance-Verpflichtungen zu erfüllen. Die Compliance-Management-Funktionalitäten in Alfabet unterstützen die Definition von Compliance-Abfragen, die Verwaltung von Compliance-Projekten,

die Bewertung von Zielobjekten im Kontext eines Compliance-Projekts sowie die Überwachung von Compliance-Projekten.

Die folgende Tabelle gibt einen Überblick über die Funktionen der einzelnen Optionen:

Funktionalität	Bewertungsmethode	Identifizieren von Anwendern zur Bewertung	Konfigurationsanforderungen
Risikomanagement	Anwender bewerten das Basis-Gefährdungspotenzial von Objekten, um die Objekte, die eine detaillierte Risikobewertung erfordern, zu priorisieren und zu fokussieren. Es können Risikominderungen definiert werden, die später durch ein Projekt realisiert werden.	Anwender werden explizit einer Risikomanagementgruppe zugeordnet.	Kennzahlensysteme und Kennzahltypen müssen konfiguriert werden.
Compliance-Management	Die Auswertung erfolgt objektweise über einen Compliance-Bewertungsassistenten. Ein Nachteil dieser Methode besteht darin, dass für die Beantwortung aller Fragen dieselbe Metrik verwendet werden muss.	Anwender werden über eine für eine Compliance-Richtlinie konfigurierte Abfrage gefunden.	Es müssen mehrere Abfragen konfiguriert und ein Indikatortyp angegeben werden.
Umfragen	Komplexe Datenerfassungsformulare stehen dem Anwender in konfigurierten Assistenten zur Verfügung. Workflows sorgen dafür, dass die Datenerfassungsmaßnahmen an die verantwortlichen Anwender verteilt und dass alle Datenerfassungsmaßnahmen zu den angegebenen Terminen abgeschlossen werden.	Anwender werden über eine für einen Workflow konfigurierte Abfrage gefunden.	Umfragen sind sehr flexibel in ihrer Konzeption, erfordern aber in der Regel eine komplexe Konfiguration, einschließlich der Konfiguration von benutzerdefinierten Klassen, benutzerdefinierten Eigenschaften, benutzerdefinierten Editoren/Assistenten und Workflows. Die Umfragen werden von einem Lösungsentwickler im Alfabet Expand Konfigurations-Tool konfiguriert und sind hier nicht beschrieben. Informationen hierzu finden Sie im Abschnitt *Konfigurieren von Umfragen für Datenerfassungskampagnen* im Referenzhandbuch *Konfigurieren von Alfabet mit Alfabet Expand*.

Folgende Informationen sind verfügbar:

- Einführung in IT-Governance, Risiko und Compliance
- Applikationsrisikomanagement
- Informationsrisikomanagement

- Projektrisikomanagement
- Compliance-Management

Kapitel 2: Applikationsrisikomanagement

Unternehmen müssen Strategien, Architekturen und Prozesse mit einem Verständnis aller möglichen relevanten Bedrohungen und Schwachstellen planen und verwalten, um Risiken zu minimieren. Alfabet bietet eine Applikationsrisikomanagement-Funktion, mit der Sie Applikationen bewerten und analysieren können, um die relevanten Bedrohungen und Risiken für die Applikationsarchitektur zu verstehen.

Ein Risiko bezieht sich auf die Wahrscheinlichkeit, mit der ein bestimmtes Objekt in der IT-Landschaft des Unternehmens einer vorhandenen Bedrohung ausgesetzt ist, und Ziel eines potentiellen Angriffs werden kann. Die Definition eines Risikos umfasst die Beurteilung des potenziellen Risikoschadens, der potenziellen Eintrittswahrscheinlichkeit des Risikos und idealerweise eine planbare und umsetzbare Risikominderung im Unternehmen. Durch die Bewertung von Risikoanträgen verstehen Sie, welche Applikationen in der Landschaft zu tolerieren sind, aber beobachtet werden müssen und welche Applikationen Risiken aufweisen, die gemindert werden müssen. Antworten auf diese Fragen zu finden, ist für die Pflege einer gesunden und kosteneffektiven Architektur sowie für die Planung künftiger Betriebsmodelle von entscheidender Bedeutung.

Die folgenden Funktionalitäten bilden die Fähigkeit des Risikomanagements:

- Der Explorer *Risikomanagementvorlagen* ermöglicht die Konfiguration von Risikoprojekten, die sich auf verschiedene Bereiche der IT konzentrieren.
- Der Explorer *Risikominderungsvorlagen* ermöglicht die Definition eines Katalogs von Risikominderungen, um die Standardisierung von Minderungen zu unterstützen.
- Die Funktionalität *Bedrohungsmanagement* ermöglicht es, einen Katalog von Bedrohungen zu definieren, um Bedrohungen und Schwachstellen mit Risiken für tatsächliche Applikationen in der IT zu verknüpfen.
- Die Funktionalität *Risikomanagement* ermöglicht die Definition von Risikomanagementgruppen mit den Applikationen, auf die das Risikoprojekt abzielt.
- Die Funktionalität *Risikodokumentation* ermöglicht es, dass das Basis-Gefährdungspotential der Applikationen überwacht und vom für die Risikobewertung verantwortlichen Anwender bewertet werden.

Damit Sie mit der Bewertung des Risikos für die Applikationsarchitektur beginnen können, müssen bereits Daten zur Applikationslandschaft erfasst und gepflegt worden sein. Die Aktivitäten im Zusammenhang mit der Datensammlung erfolgen auf der Ebene der einzelnen Applikationen und werden in der Regel von einem Applikationseigentümer oder anderen verantwortlichen Mitarbeitern koordiniert. Idealerweise wurden in Ihrem Unternehmen bereits alle relevanten Applikationen im Inventory erfasst. Informationen zu den Applikationen, wie die Business-Daten, die von ihnen übertragen werden, der technische Kontext, der für die Ausführung der Applikation erforderlich ist, die Business-Prozesse, die von der Applikation unterstützt werden, sowie die funktionalen Domänen, denen die Applikation angehört, müssen ebenfalls dokumentiert und auf dem neuesten Stand sein. Informationen zum Erfassen von Applikationsdaten finden Sie im Referenzhandbuch *Unternehmensarchitekturmanagement*.

Folgende Informationen sind über die Funktionalität "Applikationsrisikomanagement" verfügbar:

- Methodik: Risikomanagement verstehen
- Voraussetzungen: Konfigurationsanforderungen für das Risikomanagement
- Verständnis der Governance und Zuständigkeiten im Applikationsrisikomanagement

- Erfassung von Bedrohungen und Definition von Risikominderungsvorlagen
  - Definition von Bedrohungsgruppen und Erfassung von Bedrohungen
  - Angeben von Risikominderungsvorlagen für den Bedrohungskatalog
  - Verstehen der Applikationsrisiken basierend auf vorhandenen Bedrohungen
- Bewerten von Objekten für Risikorelevanz
  - Erzeugen von Risikomanagementgruppen
  - Bewertung der Relevanz von Objekten für die Risikobewertung
- Durchführung der Risikobewertung von Applikationen
  - Bewertung von Applikationen für Risiken
  - Analysieren der Risikobewertung
- Erfassen und Verwalten von Risikominderungen
- Verwalten und Speichern der Daten über die Risikobewertung

Für jede Ansicht in der Funktionalität "Applikationsrisikomanagement" steht eine kontextsensitive Hilfe zur Verfügung. In der Hilfe finden Sie Erklärungen zu den Funktionalitäten und zu den in einer bestimmten Ansicht verfügbaren Informationen.

Methodik: Risikomanagement verstehen

Um mithilfe der Risikomanagement-Funktionalität Risikoanträge beurteilen zu können, müssen die Applikationen Ihres Unternehmens in der Alfabet als Teil des IT-Bestands Ihres Unternehmens erfasst werden. Im Idealfall werden die verschiedenen Schichten der IT einschließlich der Applikations- und Informationsarchitekturen sowie der Business-Schicht dokumentiert. Die Verantwortlichkeiten für die Applikationen sollten definiert und die Beziehungen der Applikationen zu anderen Aspekten der IT-Architektur modelliert werden.

Weitere Informationen zur Dokumentation des Umfangs der IT-Inventarisierung finden Sie im Referenzhandbuch *Unternehmensarchitekturmanagement*.

Die folgenden Rollen sind typischerweise für die Risikobewertung zuständig:

- IT-Compliance-Manager
- Senior-Informationssicherheitsverantwortlicher
- Applikationseigentümer
- Prozesseigentümer und Mitwirkende

Die Risikomanagement-Funktion von Alfabet besteht in der Regel aus vier Aktivitäten, die sich darauf konzentrieren, die Bedrohungen für die IT-Architektur Ihres Unternehmens zu verstehen, die Schwachstellen von Applikationen zu bewerten und zu priorisieren, die Risiken und potenziellen Schäden an den am stärksten gefährdeten Applikationen zu bewerten und Risikominderungsmaßnahmen festzulegen und umzusetzen. Diese Methodik ermöglicht es dem Unternehmen, den Risikobewertungsprozess zu rationalisieren und

gezielt die relevanten Objekte anzusprechen, die im Unternehmen am stärksten gefährdet sind. Ein Katalog von Standardbedrohungen einschließlich Vorlagen, die Risiken und Risikominderungen beschreiben, kann für regelmäßige Bewertungen der IT wiederverwendet werden.

Abbildung: Empfohlene Prozesse für das Risikomanagement

Für das Risikomanagement in Alfabet wird die folgende Methode empfohlen:

- **Identifizieren von Bedrohungen und Festlegen von Risikominderungsvorlagen:** Bei jedem Geschäftsbereich, der beurteilt werden soll, sollte ein Anwender, der ein Risikospezialist für diesen Bereich ist (z. B. Handelsrisiken, usw.), die Bedrohungen für die Applikationen dieses Business-Bereichs darstellen können, bewerten. Bedrohungen können in Alfabet sowohl manuell erfasst als auch über das Alfabet Data Integration Framework (ADIF) aus einem Repository mit einem Katalog von Standardbedrohungen importiert werden. Für jede definierte Bedrohung können eine oder mehrere Risikominderungsvorlagen definiert werden, die darauf abzielen, das von der potenziellen Bedrohung abgeleitete Risiko zu vermeiden, zu reduzieren oder einzudämmen. Die Definition eines Katalogs von Risikominderungsvorlagen reduziert den Aufwand während der Risikobewertungsphase und unterstützt die Standardisierung der Minderungsstrategie im Unternehmen.
- **Bewertung der Risikorelevanz von Applikationen:** Um den Prozess der Erfassung der Risiken und deren Minimierung für die Applikationsarchitektur des Unternehmens zu rationalisieren, muss das Basis-Gefährdungspotential der Applikationen im Unternehmen bewertet werden. Durch die Bewertung der Risikorelevanz können die Applikationen daraufhin überprüft werden, ob potenzielle Risiken bestehen und welche Bedeutung diese haben. Für jede Applikation, die von der Risikobewertung erfasst wird, müssen Fragen beantwortet werden, um das Risiko für die Applikation zu bewerten. Alle Risikorelevanzwerte oberhalb der vorgegebenen Schwelle werden somit als relevant für den Eintritt in die nächste Phase, in der die Risiken für die Applikation näher definiert werden, angesehen.
- **Bewertung von Risiken und Schäden an Applikationen**: Diese Phase der Gefährdungsbeurteilung zielt nur auf die Objekte ab, die auf ihre Risikorelevanz hin bewertet wurden und für die eine Gefährdungsbeurteilung erforderlich ist. Die Spezifikation des Risikos umfasst die potenziellen Schadenskosten der Applikation und die Wahrscheinlichkeit einer Beschädigung der Applikation sowie Vorschläge zur Risikominimierung. Die potenziellen Schadenskosten für die Applikation und die Wahrscheinlichkeit einer Beschädigung der Applikation, wenn die vorgeschlagene Minderung umgesetzt wird, können ebenfalls dokumentiert werden. Die vorgeschlagene Minderung dient nur Informationszwecken. In der nächsten Stufe des Risikomanagements werden planbare und operationalisierbare Minderungen erfasst.
- **Risikominderungen definieren und implementieren**: Sobald die Risiken für die Applikation definiert sind, können Risikominderungen definiert werden, die verfolgt und umgesetzt werden können, um das Risiko zu vermeiden, zu reduzieren oder einzudämmen. Die Risikominderung kann auf einer vorkonfigurierten Risikominderungsvorlage basieren. Für jede Risikominderung können die Architekturelemente, die von der Risikominderung betroffen sein könnten, dokumentiert werden. Darüber hinaus kann eine Anforderung erstellt werden, in der zum Ausdruck gebracht wird, dass die Risikominderung in der IT-Architektur angegangen werden muss. Sobald die

Anforderung zur Risikominderung artikuliert wurde, kann ein Projekt erstellt werden, um die Risikominderung zu implementieren.

Um Anforderungen zu erfassen, müssen Sie Zugriff auf die Demand-Management-Funktionalität haben und um Projekte zu erfassen, müssen Sie Zugriff auf die Project Portfolio Governance-Funktionalität haben, die beide Teil des Vertriebspakets "IT Planning Advanced" sind.

Voraussetzungen: Konfigurationsanforderungen für das Risikomanagement

Für die Implementierung der **Risikomanagement** -Funktionalität in Alfabet müssen Sie Folgendes konfigurieren:

- Die Risikomanagementvorlagen müssen konfiguriert werden, um die Objektklassen anzugeben, die das Ziel der Risikobewertung sind. Die Risikomanagementvorlage umfasst die Kennzahlensysteme, die die für die **Risikobewertungsphase** zu verwendenden Fragen darstellen, die Kennzahltypen zur Definition des Risikoschadens und der Wahrscheinlichkeit eines Risikoschadens am Risikoträger in der **Risikobewertungsphase** sowie ein Risikoportfolio zur Analyse der Risikobewertung. Die Risikomanagementvorlagen werden im Explorer *Risikomanagementvorlagen* definiert.

  Es wird dringend empfohlen, dass der Anwender, der das Risikoprojekt gestaltet, einen pragmatischen qualitativen Ansatz verfolgt, der sich an die relevanten Stakeholder richtet. Die Bewertungsfragen sollten ein kompakter Satz von Fragen mit einfachen Antworten sein und die Antworten sollten zur einfachen Analyse auf numerische Werte abgebildet werden.

- Risikovorlagen können so konfiguriert werden, dass ein Standardsatz von Risiken sowie Vorschläge zur Risikominderung gruppiert werden. Ein Risiko kann explizit für einen bestimmten Risikoträger definiert oder über eine konfigurierte Risikovorlage dem Risikoträger hinzugefügt werden. Eine Risikovorlage wird über die Ansichtsseite *Risikovorlagen* definiert, die für eine klassenbasierte Risikomanagementvorlage verfügbar ist.
- Risikominderungsvorlagen können so konfiguriert werden, dass eine vordefinierte Risikominderung für eine bestimmte Bedrohung erfasst wird, um zu artikulieren, wie das von der potenziellen Bedrohung abgeleitete Risiko vermieden, reduziert oder eingedämmt werden kann. Die Risikominderungsvorlage enthält den Namen der Risikominderung, das Zieldatum, an dem die Risikominderung umgesetzt werden soll, und eine Anzahl von Prioritäten für die Risikominderung. Die Risikominderung kann dann für ein Risiko-Objekt im Rahmen einer Risikobewertung definiert werden. Risikominderungsvorlagen werden über den Explorer *Risikominderungsvorlagen* definiert.

Detaillierte Beschreibung der Konfiguration von Risikomanagementvorlagen, Risikovorlagen und Risikominderungsvorlagen finden Sie im Abschnitt *Konfigurieren der Funktionalität „Risikomanagement“* im Referenzhandbuch *IT-Governance, Risiko und Compliance*.

Verständnis der Governance und Zuständigkeiten im Applikationsrisikomanagement

In der Funktionalität "Applikationsrisikomanagement" sind verschiedene Steuerungskonzepte implementiert:

- **Risiko-Objekt**: Jede Applikation, die einer Risikomanagementgruppe zugeordnet ist, wird als Risiko-Objekt definiert. Die Risikobewertung und Bewertung der Applikation werden nur für das Risiko-Objekt angegeben. Das Risiko-Objekt hat seine eigene Definition eines **autorisierten Anwenders**, die sich von der Definition des **autorisierten Anwenders** der Applikation unterscheiden kann, auf der das Risiko-Objekt basiert. Die Risikobewertung ist daher nur für Anwender in der Anwendergemeinschaft sichtbar, die die Autorisierung für das Risiko-Objekt haben.
- **Rollen**: Über eine Rolle wird die funktionale Beziehung oder Verantwortlichkeit eines Anwenders oder einer Organisation bezüglich einer Applikation oder eines Risiko-Objekts definiert (beispielsweise als Risikomanager oder Architekt einer Applikation). Das Risiko-Objekt verfügt über eine eigene Rollendefinition, die sich von der Rollendefinition der Applikation, die dem Risiko-Objekt zugrunde liegt, unterscheiden kann. Rollen beschreiben Zuständigkeiten, aber sie berechtigen nicht zu Zugriffsberechtigungen auf die Applikation in Alfabet.
- **Mandanten**: Risikomanagementgruppen können in einer Partner-Architektur verwaltet werden. Mithilfe einer Partnerarchitektur kann die Sichtbarkeit einzelner Risikomanagementgruppen auf der Benutzeroberfläche von Alfabet für bestimmte Anwender festgelegt werden.

Erfassung von Bedrohungen und Definition von Risikominderungsvorlagen

Mit einer **Bedrohungsmanagement** -Funktion können Sie das Risiko für die Unternehmens-IT ermitteln, planen und mindern. Die Bewertung von Bedrohungen unterstützt das Unternehmen dabei, den Wert des Applikationsportfolios zu erkennen, Risiken für die Applikationsarchitektur effektiv zu bewerten und zu mindern und damit verbundene Projekte zur Risikominderung zu planen.

Bei jedem Geschäftsbereich, der beurteilt werden soll, sollte ein Anwender, der ein Risikospezialist für diesen Bereich ist (z. B. Projektrisiken, Handelsrisiken, usw.), die Bedrohungen beurteilen, die Risiken für diesen Bereich darstellen können. Eine Bedrohung verweist auf die Quelle eines bestimmten Risikotyps und kann mit einem oder mehreren Risiko-Objekten in der IT-Landschaft des Unternehmens verbunden werden. Bedrohungen können in Alfabet entweder manuell erfasst oder über das Alfabet Data Integration Framework (ADIF) aus einem Repository wie zum Beispiel der National Vulnerability Database (NVD) des National Institute of Standards and Technology (NIST) importiert werden.

Der Import von Bedrohungen aus einem Repository oder einer anderen Datenbank erfordert die Funktion „Alfabet Data Integration Framework (ADIF)“, die über das Konfigurationstool Alfabet Expand verfügbar ist. Weitere Informationen zu ADIF finden Sie im Referenzhandbuch *Alfabet-Datenintegrationsframework*.

In Alfabet verweist eine Bedrohung auf die Quelle einer bestimmten Art von Risiko für die IT des Unternehmens. Bedrohungen können im Rahmen von hierarchisch gegliederten Bedrohungsgruppen organisiert und bewertet werden. Für jede definierte Bedrohung können eine oder mehrere Risikominderungsvorlagen definiert werden, die darauf abzielen, das von der potenziellen Bedrohung abgeleitete Risiko zu vermeiden, zu

reduzieren oder einzudämmen. Die Risikominderungsvorlage kann später von Anwendern verwendet werden, wenn spezifische Minderungen für tatsächliche Risiken definiert werden. Wenn ein Risiko für eine Applikation bewertet wird, kann das Risiko auf einer bestehenden Bedrohung beruhen, die bereits in Alfabet dokumentiert wurde. Das Risiko erbt die Risikominderung auf der Grundlage der Risikominderungsvorlage, die für die Bedrohung, von der das Risiko abgeleitet wird, definiert wurde.

Die Definition eines Katalogs von Risikominderungsvorlagen reduziert den Aufwand während der Risikobewertungsphase und unterstützt die Standardisierung der Minderungsstrategie im Unternehmen.

Folgende Informationen sind verfügbar:

- Definition von Bedrohungsgruppen und Erfassung von Bedrohungen
- Angeben von Risikominderungsvorlagen für den Bedrohungskatalog
- Verstehen der Applikationsrisiken basierend auf vorhandenen Bedrohungen

Definition von Bedrohungsgruppen und Erfassung von Bedrohungen

Bedrohungsgruppen bündeln eine Reihe von Bedrohungen. Bedrohungsgruppen sollten auf der Grundlage der in Ihrem Unternehmen verwendeten Risikobewertungsmethode definiert werden. Bedrohungen können entweder manuell definiert oder ein Katalog von standardisierten Bedrohungsgruppen und Bedrohungen über ADIF importiert werden.

Abbildung: Bedrohungsgruppenhierarchie mit Bedrohungen auf Blattebene

Das obige Beispiel zeigt eine Bedrohungsgruppenhierarchie für Microsoft® Internet Explorer®. Die untergeordneten Bedrohungsgruppen repräsentieren jede IE-Version und die Bedrohungen für eine IE-Version werden auf Blattebene der untergeordneten Bedrohungsgruppe angezeigt. In diesem Fall wurden die Bedrohungen aus einem Repository importiert. Das Attribut **Beschreibung** im Objektprofil der Bedrohung erfasst die Informationen über die Bedrohung. Beachten Sie Folgendes:

- Die Hierarchie der Bedrohungsgruppe kann manuell in der Funktionalität *Bedrohungsmanagement* erstellt werden.
- Bedrohungen können auf der Ansichtsseite *Bedrohungen* für jede Bedrohungsgruppe in der Hierarchie erfasst werden. Die Bedrohung sollte einen Namen, einen Release-Status und eine Beschreibung aufweisen.

Angeben von Risikominderungsvorlagen für den Bedrohungskatalog

Die Risikominderungen können geplant und implementiert werden, um potentiellen Bedrohungen zu begegnen sowie Risiken für die IT-Landschaft zu vermeiden, zu reduzieren oder einzudämmen. Mit Risikominderungsvorlagen können Risikominderungen standardisiert und konsistente Daten für eine Reihe von Risiko-Objekten erfasst werden.

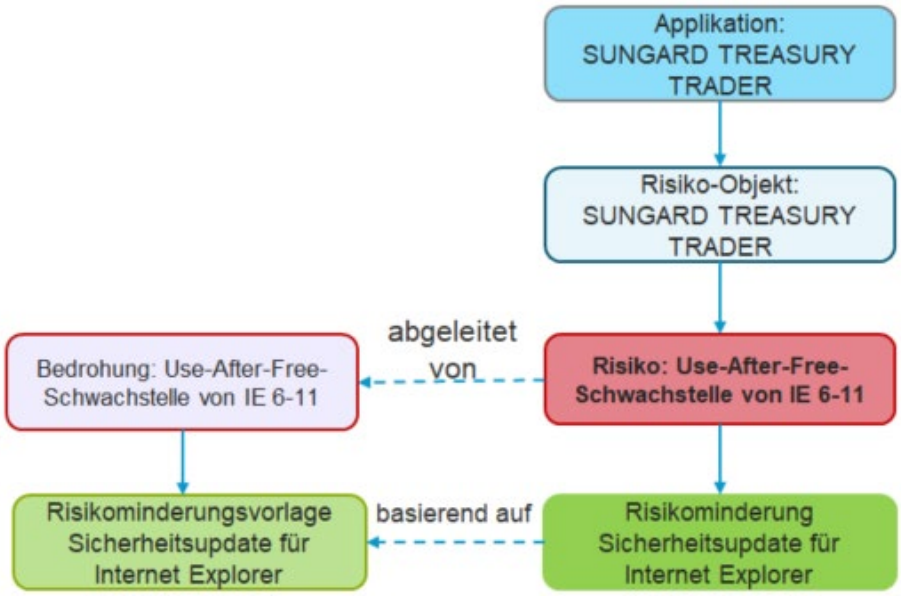


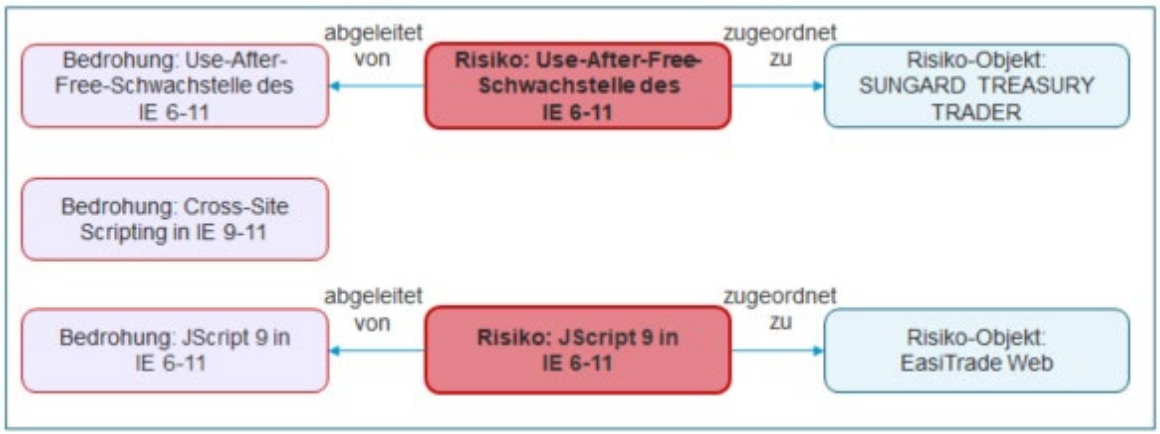
Abbildung: Risikominderung basierend auf einer für die Bedrohung definierten Risikominderungsvorlage

Wenn ein Risiko für eine Applikation bewertet wird, kann das Risiko auf einer bestehenden Bedrohung beruhen, die bereits in Alfabet dokumentiert wurde. Das Risiko erbt die Risikominderung auf der Grundlage der Risikominderungsvorlage, die für die Bedrohung, von der das Risiko abgeleitet wird, definiert wurde. Die Definition eines Katalogs von Risikominderungsvorlagen reduziert den Aufwand während der Risikobewertungsphase und unterstützt die Standardisierung der Minderungsstrategie im Unternehmen.

Eine Risikominderungsvorlage erfasst eine vorkonfigurierte Definition einer Minderung, die für eine bestimmte Bedrohung gilt. Die Definition einer Risikominderungsvorlage enthält den Namen der Risikominderung, das Zieldatum, an dem die Risikominderung umgesetzt werden soll, und eine Anzahl von Prioritäten für die Risikominderung. Wenn ein Risiko für eine Applikation im Rahmen einer Risikobewertung spezifiziert wird, kann das Risiko auf einer vorhandenen Bedrohung basieren, die Teil des Bedrohungs- und Schwachstellenkatalogs des Unternehmens ist. Die Risikominderungsvorlage wird dann als Risikominderung in das Risiko übernommen. Die Definition der Risikominderung kann nach Bedarf geändert werden.

Risikominderungsvorlagen für eine Bedrohung werden auf der Ansichtsseite *Risikominderungsvorlage* der entsprechenden Bedrohung definiert.

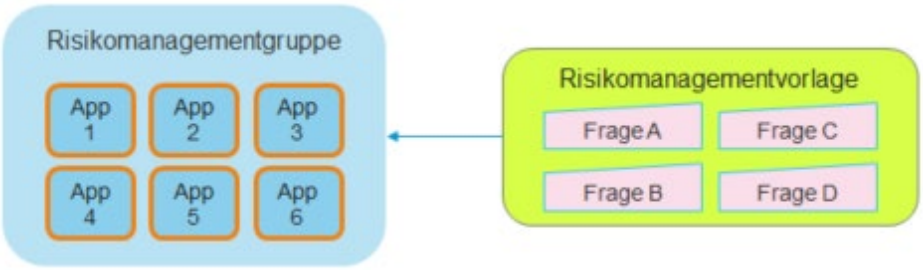
Verstehen der Applikationsrisiken basierend auf vorhandenen Bedrohungen



Auf der Ansichtsseite *Zugehörige Risiken* werden alle Risiko-Objekte angezeigt, die aus der ausgewählten Bedrohung abgeleitet wurden. Der Bericht enthält Informationen über die Risiko-Objekte und ihre definierten Risiken, einschließlich der potenziellen Schadenskosten für die Applikation und der Wahrscheinlichkeit einer Beschädigung der Applikation, wenn das Risiko eintritt und wenn das Risiko gemindert werden soll.

Bewerten von Objekten für Risikorelevanz

Bevor die Applikationen auf Risiken geprüft werden, sollten sie priorisiert werden, um festzustellen, welche Applikationen am wichtigsten zu schützen sind. Um den Prozess der Erfassung der Risiken und deren Minimierung für die Applikationsarchitektur des Unternehmens zu rationalisieren, muss das Basis-Gefährdungspotential der Applikationen im Unternehmen bewertet werden. Das Basis-Gefährdungspotential ist eine Bewertung von Applikationen entsprechend ihrer potentiellen Risiken. Jede Applikation, die bewertet werden soll, muss einer Risikomanagementgruppe zugewiesen werden, dabei wird sie anhand eines Risikorelevanz-Fragebogens bewertet.



Die Fragen zur Ermittlung der Risikorelevanz werden typischerweise von einem für die Risikobewertung verantwortlichen Anwender in Ihrem Unternehmen erstellt. Die Fragen werden in einer Risikomanagementvorlage konfiguriert, die für die Risikomanagementgruppe angegeben wird, die die zu bewertenden Applikationen enthält. Jede Applikation, die einer Risikomanagementgruppe zugeordnet ist, wird als Risiko-Objekt betrachtet. Es handelt sich um das Risiko-Objekt, das im Rahmen des Risikomanagements bewertet wird. Dadurch wird sichergestellt, dass diese Informationen nur für Anwender in der Anwendergemeinschaft sichtbar sind, die Zugriff auf das Risiko-Objekt haben.

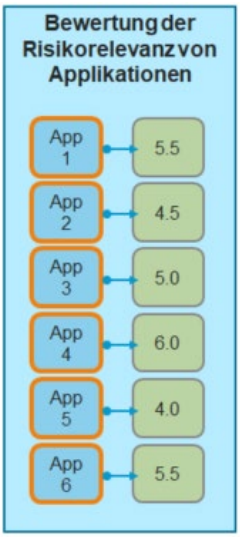


Abbildung: Applikationen mit ihren Risikorelevanzwerten

Für jede Applikation, die von der Risikobewertung erfasst wird, müssen konfigurierte Fragen beantwortet werden, um das Risiko für die Applikation zu bewerten. Ein Prozessverantwortlicher evaluiert die Applikationen idealerweise, indem er für jede Applikation einen konfigurierten Satz von Fragen beantwortet, um eine Bewertung zu erstellen, die die Relevanz des Risikos für jede Applikation bestimmt. Die Antworten auf alle Fragen zur Applikation werden berechnet, um einen Risikorelevanzwert zu generieren. Dieser Risikorelevanzwert gibt die Risikostufe für die Applikation an.

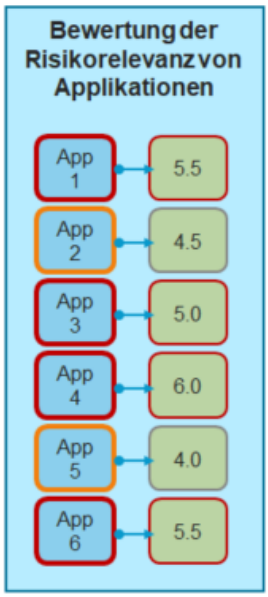


Abbildung: Der Schwellenwert für die Risikorelevanz ist auf 5 festgelegt.

Nachdem alle Applikationen ausgewertet wurden, kann ein Schwellenwert definiert werden.

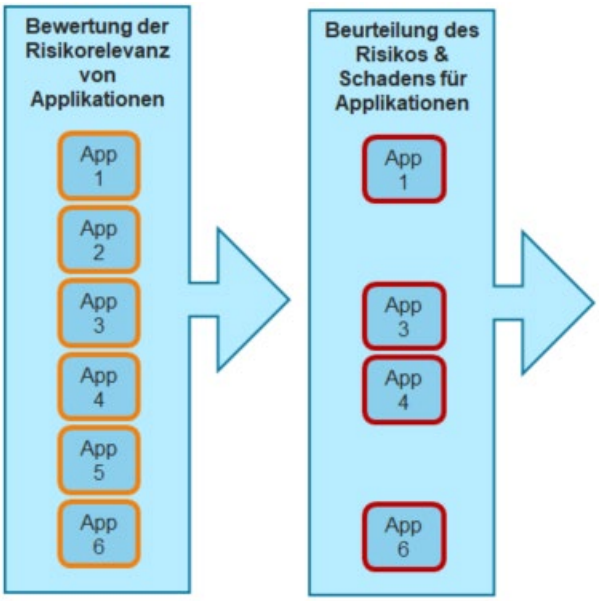


Abbildung: Applikationen, die über dem Schwellenwert liegen, werden für das Risiko bewertet.

Alle Risikorelevanzwerte, die gleich oder über dem angegebenen Schwellenwert sind, sollten an die Risikobewertungsphase gesendet werden, in der die Risiken für die App im Detail definiert sind.

Folgende Informationen sind verfügbar:

- Erzeugen von Risikomanagementgruppen
- Bewertung der Relevanz von Objekten für die Risikobewertung

Erzeugen von Risikomanagementgruppen

Eine Risikomanagementgruppe ist ein Container zur logischen Strukturierung der Applikationen, die bewertet werden. Alle Risikomanagementgruppen können eine eigene Risikomanagementvorlage haben, um verschiedene Perspektiven zur Strukturierung und Analyse von Risiko-Objekten nutzen zu können. Die der Risikomanagementgruppe zugeordnete Risikomanagementvorlage legt Folgendes fest:

- Die Objektklassen, die für das Risikoprojekt vorgesehen werden können.
- Die Fragen, die zu beantworten sind, um das Basisrisiko der Risikomanagementgruppe zugeordneten Applikationen zu bewerten.
- Die Kennzahltypen für die Risikominderung und Risikowahrscheinlichkeit, die eine Dokumentation der aus dem Risiko und der Risikominderung resultierenden potenziellen Kosten ermöglichen.
- Das Risiko- Portfolio, das zur Analyse der Risiken für die Applikationen in der Risikomanagementgruppe verfügbar ist.
- Die Risikovorlagen, die zur Definition der Risiken für die Applikationen in der Risikomanagementgruppe verfügbar sind.

Eine Applikation kann mehreren Risikomanagementgruppen zugeordnet werden, wodurch ein und dasselbe Risiko-Objekt in verschiedenen Zusammenhängen betrachtet werden kann.

Eine Risikomanagementgruppe wird in der Funktionalität *Risikomanagement* erzeugt. Gegebenenfalls können Sie untergeordnete Risikomanagementgruppen erzeugen. Für jede Risikomanagementgruppe muss ein Name, eine Beschreibung und eine Risikomanagementvorlage definiert werden.

Alle Applikationen, deren Basis-Gefährdungspotential bewertet werden soll, sollten der Risikomanagementgruppe in der Ansichtsseite *Zugehörige Objekte* der Risikomanagementgruppe zugewiesen werden.

Bewertung der Relevanz von Objekten für die Risikobewertung

Die Funktionalität *Risikodokumentation* zeigt alle Risiko-Objekte an, für die ein Anwender als autorisierter Anwender oder durch die Anwendergruppen verantwortlich ist, in denen er/sie Mitglied ist. Diese Funktion ermöglicht den Zugriff auf die Ansichtsseite *Risikorelevanz-Fragenkatalog* sowie die Ansichtsseite *Risikobewertung*.

Die Fragen in der Ansichtsseite *Risikorelevanz-Fragenkatalog* müssen für jede Applikation in der Risikomanagementgruppe beantwortet werden, um eine Risikorelevanzbewertung für Ihr Basis-Gefährdungspotential zu ermitteln. Für jede Frage, die Sie beantworten, wird ein Wert einem Kennzahltyp zugeordnet, der ein relevantes Problem für die Risikobewertung darstellt.

Für eine GDPR-Risikobewertung können die folgenden Fragen (Kennzahltypen) und Antworten (Wertebereich) relevant sein, um zu ermitteln, ob eine Applikation in der Risikobewertung berücksichtigt werden soll.

Frage	Antwort
Daten anonymisiert?	• 1 - Ja • 2 - Nein
Daten verschlüsselt?	• 0 - Vollständig verschlüsselt • 1 - Teilweise verschlüsselt • 2 – Nicht verschlüsselt
Aufbewahrungsfrist der verarbeiteten Daten	• 1 - < 3 Jahre • 2 - zwischen 3 und 30 Jahren • 3 - > 30 Jahre

Die Kennzahltypen **Datenzunahme**, **Datenempfindlichkeit** und **Risiko eines Datenlecks** wurden als Aspekte der Relevanz für die GDPR-Risikobewertung konfiguriert. Wenn eine Frage bezüglich der Auswirkungen von **Daten anonymisiert?** für eine Applikation mit der Option **2 - Nein** beantwortet wird, dann kann der Wert 0 (sehr niedrige Bewertung) für den Kennzahltyp **Datenzunahme** sein, aber 4 (sehr hohe Punktzahl) für den Kennzahltyp **Risiko eines Datenlecks** sein.

Die Antworten auf alle Fragen werden allen Kennzahltypen zugeordnet, die für die Risikobewertung relevant sind. All diese Werte werden zusammen hinzugefügt, um einen Risikorelevanzwert für die Applikation zu erzielen, mit deren Hilfe das Basis-Gefährdungspotential bestimmt wird.

Die Fragen und Antworten, die Kennzahltypen, die die Relevanz für die Risikobewertung darstellen, und die Zuordnung von Antworten zu den Kennzahltypen werden auf der Ansichtsseite *Konfigurieren von Risikomanagementvorlagen für die Funktionalität „Risikomanagement“* konfiguriert.

Die Risikorelevanzwerte werden für alle Applikationen in der Risikomanagementgruppe auf der *Zugehörige Objekte* angezeigt. Je höher der Risikorelevanzwert der Applikation ist, desto höher ist das Basis-Gefährdungspotential der Applikation. Um zu bestimmen, welche Applikationen in der Risikobewertung berücksichtigt werden sollen, kann ein Schwellenwert im Feld **Risikorelevanzwert** definiert werden. Alle Objekte, die einen Risikorelevanzwert aufweisen, der dem eingegebenen Wert entspricht oder diesen überschreitet, werden markiert. Idealerweise handelt es sich dabei um die Objekte, die die höchste Priorität für die Risikobewertung haben. Unabhängig von den in der **Risikorelevanzbewertung** definierten Schwellenwerten kann jedes Risiko-Objekt auf der *Risikobewertung* für das Risiko im Risiko-Objekt bewertet werden.

Durchführung der Risikobewertung von Applikationen

Die Applikationen in der Risikomanagementgruppe, die einen Risikorelevanzwert für das Basis-Gefährdungspotential haben, haben die höchste Priorität, für Risiken bewertet zu werden. Unabhängig von den in der **Risikorelevanzbewertung** definierten Schwellenwerten kann jedes Risiko-Objekt auf der Ansichtsseite *Risikobewertung* für das Risiko im Risiko-Objekt bewertet werden. Diese Phase der Gefährdungsbeurteilung zielt jedoch idealerweise nur auf die Objekte ab, die auf ihre Risikorelevanz hin bewertet wurden und für die eine Gefährdungsbeurteilung erforderlich ist.

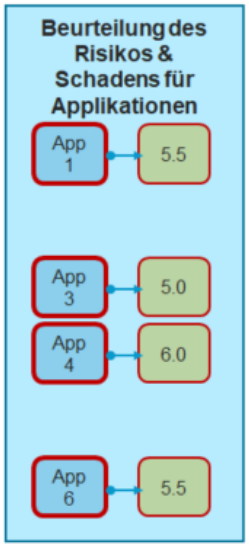


Abbildung: Applikationen für die Risikobewertung

Für jede Applikation in der Risikobewertung können ein oder mehrere Risiken definiert werden. Die Risiken können manuell definiert werden, basierend auf dem Katalog der Bedrohungen im Inventory oder aus einer vorkonfigurierten Risikovorlage.

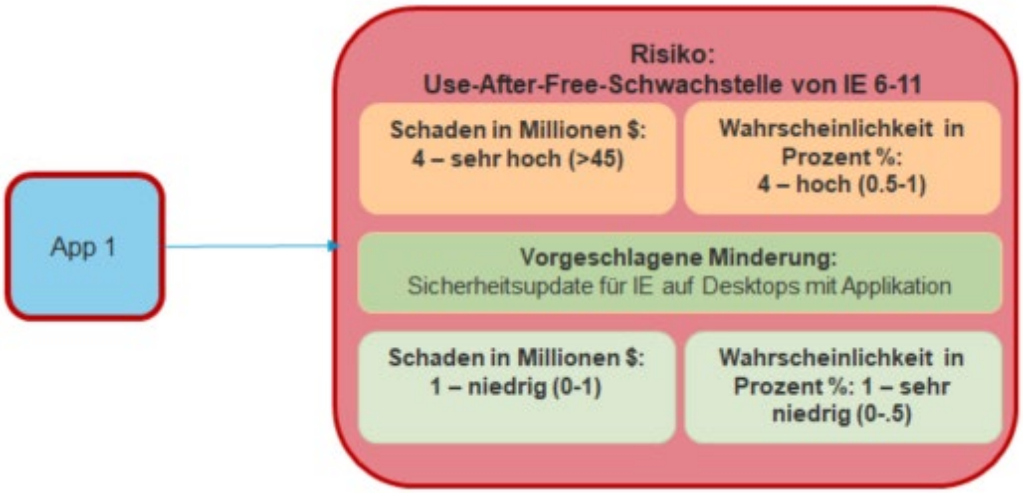


Abbildung: Risikodefinition einschließlich möglicher Kosten und Kosten nach Risikominderung

Die Spezifikation des Risikos umfasst die potenziellen Schadenskosten der Applikation und die Wahrscheinlichkeit einer Beschädigung der Applikation sowie Vorschläge zur Risikominimierung. Die potenziellen Schadenskosten für die Applikation und die Wahrscheinlichkeit einer Beschädigung der Applikation, wenn die vorgeschlagene Minderung umgesetzt wird, können ebenfalls dokumentiert werden. Die vorgeschlagene Minderung dient nur Informationszwecken. In der nächsten Stufe des Risikomanagements werden planbare und operationalisierbare Minderungen erfasst.

Bewertung von Applikationen für Risiken

Definieren Sie auf der Ansichtsseite Risikobewertung für jedes Objekt in der Risikomanagementgruppe, das einen hohen Risikorelevanzwert aufzeigt, ein oder mehrere potentielle Risiken für das Objekt auf der Ansichtsseite *Risikobewertung*. Risiken können entweder von Grund auf neu definiert oder auf Grundlage eines Risikos erstellt werden, das bereits für eine andere Applikation in der Risikomanagementgruppe definiert wurde. Risiken, die von einem anderen Risiko-Objekt kopiert werden, können bei Bedarf geändert werden.

Risiken können auch für die Applikation definiert werden, indem Sie eine Risikovorlage auswählen, die mit der Risikomanagement-Vorlage verknüpft ist, die zur Risikomanagementgruppe zugeordnet wurde. Risikovorlagen bündeln einen Standardsatz von Risiken und, falls relevant, die vorgeschlagenen Risikominderungen für das Risiko-Objekt. Risiken, die der Applikation über eine Risikovorlage hinzugefügt wurden, die nicht relevant sind, können aus der Applikation gelöscht werden.

Sobald dem ausgewählten Risiko-Objekt ein Risiko zugeordnet wird, können Sie das Risiko beschreiben und einen Wert für den potentiell durch das Risiko verursachten Schaden sowie für dessen Eintrittswahrscheinlichkeit definieren. Ferner können Sie Aktionen vorschlagen, die ein Risiko potenziell mindern und einen Wert für den potenziell durch das Risiko verursachten Schaden und dessen Eintrittswahrscheinlichkeit unter Berücksichtigung der Implementierung risikomindernder Maßnahmen definieren können.

Weitere Informationen zum Erzeugen einer Risikominimierung für das Risiko, das verfolgt und implementiert werden kann, finden Sie im Abschnitt Erfassen und Verwalten von Risikominderungen.

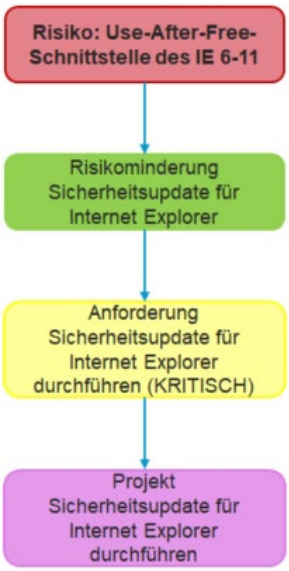
Analysieren der Risikobewertung

Die für Risikomanagementgruppen verfügbare Ansichtsseite *Risiko-Objektportfolio* hilft Ihnen, zu verstehen, welche Applikationen der Gruppe am meisten gefährdet sind. Im Bericht wird ein Portfolio angezeigt, das alle Risiko-Objekte, die der ausgewählten Risikomanagementgruppe zugeordnet sind, analysiert. Sie können die Objekte auf Basis der definierten Werte für Risikoschaden und Risiko wahrscheinlich, wenn das Risiko nicht gemindert wird, sowie der geschätzten Risikoschadens- und Risikowahrscheinlichkeit anzeigen, wenn die vorgeschlagenen Minderungsmaßnahmen umgesetzt werden sollen.

Mit der Ansichtsseite *Risikoportfolio* für ein Risiko-Objekt können Sie nachzuvollziehen, welche der Risiken den größten Schaden und die höchste Eintrittswahrscheinlichkeit in sich bergen. In dem angezeigten Bericht wird ein Portfolio angezeigt, in dem die Werte für den risikobedingten Schaden und dessen Eintrittswahrscheinlichkeit für das ausgewählte Risiko-Objekt angegeben werden.

Erfassen und Verwalten von Risikominderungen

Für jedes Risiko, das für ein Risiko-Objekt definiert ist, kann eine Risikominimierung definiert werden, um Risiken für die IT-Landschaft zu vermeiden, zu reduzieren oder einzudämmen. Die Risikominderung beschreibt einen Schritt, um ein Risiko zu vermeiden, zu mindern oder einzudämmen. Für jede Risikominderung können die Architekturelemente, die von der Risikominderung betroffen sein könnten, dokumentiert werden. Darüber hinaus kann eine Anforderung erstellt werden, in der zum Ausdruck gebracht wird, dass die Risikominderung in der IT-Architektur angegangen werden muss. Sobald die Anforderung zur Risikominderung artikuliert wurde, kann ein Projekt erstellt werden, um sie zu implementieren.



Risikominderungen können auf der Ansichtsseite *Risikominderung* für ein Risiko, dass mit einem Risiko-Objekt verbunden ist, erfasst werden. Risikominderungen können als neue Objekte erfasst werden oder auf Basis einer Risikominderungsvorlage erzeugt werden. Risikominderungen beinhalten eine Beschreibung der Minderung, ein Zieldatum, an dem die Risikominderung implementiert sein sollte, sowie die Priorisierung der Risikominderung.

Sie können in der IT-Landschaft die Architekturobjekte definieren, auf die sich die Risikominderung auswirkt. Die Architekturelemente, die von der Risikominderung betroffen sein können, werden auf der Ansichtsseite *Betroffene Architektur* im Objektprofil der Risikominderung dokumentiert. Wenn die Risikominderung von einer Risikominderungsvorlage abgeleitet wird, erbt sie von dieser automatisch den

Architekturzusammenhang. Ein betroffenes Architekturelement kann auf einer der folgenden Objektklassen basieren: Applikation, Businessdaten, Business-Funktion, Business-Objekt, Business-Prozess, Komponente, Kundensegment, Gerät, Domäne, ICT-Objekt, Informationsfluss, Marktprodukt, Masterplattform, Organisation, Externes System, Vertriebskanal, Service-Produkt, Lösungsbaustein, Standardplattform, Technologie und Anbieterprodukt.

Außerdem können auf der Ansichtsseite *Anforderungen* im Objektprofil der Risikominderung ein oder mehrere Anforderungen für die Risikominderung erzeugt werden. Die betroffene Architektur der Risikominderung wird von der Anforderung geerbt. Die Anforderungen können dann einem Projekt zugewiesen werden, dass dazu dient, die Risikominderung umzusetzen und zu implementieren.

Um Anforderungen zu erfassen, müssen Sie Zugriff auf die Demand-Management-Funktionalität haben und um Projekte zu erfassen, müssen Sie Zugriff auf die Project Portfolio Governance-Funktionalität haben, die beide Teil des Vertriebspakets "IT Planning Advanced" sind.

Wählen Sie das Risiko in der Tabelle aus, um dessen Objektprofil aufzurufen. Sie können die Risikominderung auf der Ansichtsseite *Risikominderung* erzeugen. Später können Sie in der IT-Landschaft die Architekturobjekte definieren, auf die sich die Risikominderung auswirkt, und eine auf der Risikominderung basierende Anforderung spezifizieren.

Verwalten und Speichern der Daten über die Risikobewertung

Ein Datensatz der Risikoanalyse und -bewertung für eine Risikomanagementgruppe kann gespeichert und archiviert werden. Zu jedem Zeitpunkt während der Beurteilungs- oder Bewertungsphase kann eine Momentaufnahme von allen Applikationen erzeugt werden, die einer ausgewählten Risikomanagementgruppe auf derAnsichtsseite *Zugehörige Objekte* einer Risikomanagementgruppe zugeordnet sind. Die Momentaufnahmen werden auf der Ansichtsseite *Risikomanagement-Momentaufnahmen* der ausgewählten Risikomanagementgruppe gespeichert. Für eine ausgewählte Risikomanagementgruppe kann eine unbegrenzte Anzahl von Momentaufnahmen erzeugt werden. Alle Momentaufnahmen, die nicht mehr erforderlich sind, können gelöscht werden.

Die Momentaufnahme zeichnet die Daten auf, die in der Risikobewertung aller Risiko-Objekte erfasst wurden, die der ausgewählten Risikomanagementgruppe zugeordnet sind. Der Name der Momentaufnahme wird automatisch generiert und umfasst den Namen der Risikomanagementgruppe sowie den Zeitstempel zur Angabe des Datums und der Zeit der Momentaufnahme (z. B.: Market Data_04062009_112030).

- Im ersten Teil der Momentaufnahme werden der Name der Risikomanagementgruppe und die Daten der Ansichtsseite *Zugehörige Objekte* angezeigt.
- In den nachfolgenden Abschnitten der Momentaufnahme wird die Risikorelevanzbewertung der Applikationen in der Risikomanagementgruppe angezeigt. Dort sind die Daten der Ansichtsseite *Risikorelevanz-Fragenkatalog* und der Ansichtsseite *Risikobewertung* der einzelnen Risiko-Objekte zu finden.
- Die Microsoft Excel -Datei in Excel kann mit der Funktionalität **Speichern** auf Ihrem Netzlaufwerk gespeichert werden.

Kapitel 3: Informationsrisikomanagement

Businessdaten sind die Hauptpfeiler aller großen Unternehmen und müssen vor neuen Bedrohungen und Risiken geschützt werden. Darüber hinaus verlangen neu entstehende juristische Einheiten und Vorschriften wie die Datenschutz-Grundverordnung (DSGVO), dass Unternehmen die Daten, die sie speichern und verarbeiten, kennen, zuverlässige Aufzeichnungen über ihre Verarbeitungstätigkeiten führen, die Einhaltung der Vorschriften für die Behörden nachweisen und die Nachhaltigkeit der Einhaltung gewährleisten.

Das Informationsrisikomanagement hilft dem Unternehmen, die mit den über den Informationsfluss übertragenen Daten verbundenen Risiken zu verstehen, nachzuvollziehen, ob ein kritischer Bedarf an Datenschutz besteht, und die Daten in einer Weise zu verwalten, die den Vorschriften entspricht. Die Funktionalitäten für das **Risikomanagement**, die im Abschnitt Applikationsrisikomanagement beschrieben sind, sind gleichermaßen relevant für die Beurteilung und Bewertung der Risiken für Informationsflüsse zwischen Applikationen sowie den übertragenen Businessdaten. Wie im Beispiel für die Risikobewertung von Applikationen beschrieben, können Risikomanagementvorlagen so konfiguriert werden, dass sie auf die Klasse Informationsfluss oder Businessdaten abzielen, um eine Risikobewertung und Risikobewertung der Informationsarchitektur anzustoßen.

Neben der Durchführung einer Risikobewertung zur Erfüllung der Sicherheitsanforderungen in Bezug auf das Risiko für die IT können Datenhaltungsrichtlinien so konfiguriert werden, dass sie die Speicherung und Verwaltung von Businessdaten dokumentieren, um die Einhaltung der Richtlinien zur Datenpersistenz und der gesetzlichen Archivierungsanforderungen sicherzustellen. Datenaufbewahrungsrichtlinien ermöglichen die Dokumentation von Standardinformationen darüber, wie Businessdaten aufbewahrt und gespeichert werden sollen. Die Datenaufbewahrungsrichtlinie wird den Businessdaten als Teil der Businessdatennutzungsdefinition zugeordnet.

Damit Sie mit der Bewertung des Risikos für die Informationsarchitektur beginnen können, müssen bereits Daten zur Informationslandschaft erfasst und gepflegt worden sein. Die Aktivitäten im Zusammenhang mit der Datensammlung erfolgen auf der Businessdatenebene und werden in der Regel von einem Applikationseigentümer oder anderen verantwortlichen Mitarbeitern koordiniert. Idealerweise wurden alle relevanten Applikationen, die Businessdaten, die von diesen Applikationen übertragen werden, und die Businessdatennutzung (CRUD) bereits im Inventory erfasst. Detaillierte Informationen zum Erfassen der Businessdaten finden Sie im Kapitel *Informationsarchitekturdefinition* des Referenzhandbuchs *Unternehmensarchitekturmanagement*. Weitere Informationen zum Spezifizieren und Analysieren der Businessdatennutzung finden Sie im Kapitel *Informationsportfoliosteuerung* im Referenzhandbuch *Portfoliomanagement - grundlegend*.

Implementierung von Datenaufbewahrungsrichtlinien als Teil des Informationsrisikomanagements:

- Die Datenaufbewahrungsrichtlinien müssen auf der *Ansichtsseite „Datenaufbewahrungsrichtlinien“* konfiguriert werden. Für jede erzeugte Datenaufbewahrungsrichtlinie muss Folgendes angegeben werden:
  - Eine Beschreibung der Datenaufbewahrungsrichtlinie.
  - Eine Beschreibung, wann die Datenaufbewahrungsrichtlinie beginnen soll. Zum Beispiel 3 Monate nach dem Tod, ein Jahr nach der letzten gültigen Transaktion.
  - Der Zeitraum, in dem die Businessdaten vom Unternehmen gespeichert werden sollen. Zum Beispiel 1 Monat, 6 Monate, 1 Jahr, 3 Jahre, 10 Jahre, etc.
  - Die Regeln für die Archivierung der Businessdaten. Zum Beispiel: Sofortarchivierung erforderlich, verzögerte Archivierung erlaubt, etc.

- Die zulässigen Mittel zur Speicherung der Businessdaten. Zum Beispiel: Diskette, Band, verzögert betriebsbereite Standby-Lösung, unmittelbar betriebsbereite Standby-Lösung, etc.
- Die zulässigen Mittel zum Zugriff auf die Businessdaten. Zum Beispiel: strafrechtliche Ermittlungen, Polizei, Recht, interne Prüfung, externe Prüfung, Vorstand, etc.
- Der Mindestverschlüsselungsgrad für die Businessdaten. Zum Beispiel erweiterte Verschlüsselungsstandards (AES) usw.

Datenaufbewahrungsrichtlinien werden durch Ihr Unternehmen in der Funktionalität **Referenzdatendefinition** im Modul **Konfiguration** konfiguriert. Informationen hierzu finden Sie im Abschnitt *Konfigurieren von Datenaufbewahrungsrichtlinien* im Referenzhandbuch *Konfigurieren von Bewertungen und Referenzdaten in Alfabet*.

- Die Datenaufbewahrungsrichtlinie muss den Businessdaten als Teil der Businessdatennutzungsdefinition zugeordnet werden. Die Datenaufbewahrungsrichtlinie, die für die Businessdaten oder das Business-Objekt relevant ist, wird im Editor **Nutzung von Businessdaten** auf der Ansichtsseite *Businessdaten* der entsprechenden Applikation oder Komponente ausgewählt.

Kapitel 4: Projektrisikomanagement

Der Erfolg des operativen Projektmanagements ist ein integraler Bestandteil der Fähigkeit eines Unternehmens, seine Dienstleistungen kostengünstig und zuverlässig bereitzustellen. Die Bewertung der Projektrisiken während der Durchführung des Projekts ist mit der Verwaltung des Projektportfolios verbunden. Die Projektrisikomanagement-Funktion konzentriert sich auf die Ermittlung und Bewertung der Risiken für das Projekt, die Verwaltung dieser Risiken, um die Auswirkungen auf das Projekt zu minimieren und eine effiziente Projektabwicklung und somit die Geschäftskontinuität sicherzustellen.

Die Projektrisikomanagement-Funktion unterstützt das Unternehmen dabei, die mit Projekten verbundenen Risiken zu verstehen. Die Funktionalitäten für das **Risikomanagement**, die im Abschnitt Applikationsrisikomanagement beschrieben werden, sind ebenso relevant für die Beurteilung und Bewertung der Risiken für Projekte. Wie im Beispiel für die Risikobewertung von Applikationen beschrieben, können Risikomanagementvorlagen so konfiguriert werden, dass sie sowohl auf die Klasse Projekt als auch auf einen beliebigen Projekt-Stereotyp abzielen, um eine Risikobeurteilung und Risikobewertung der Informationsarchitektur anzustoßen.

Zusätzlich zur Implementierung einer Risikobewertung, um das erfolgreiche Ergebnis der operativen Projektplanung ihres Unternehmens sicherzustellen, bietet Alfabet Projektverfolgungsfunktionen zur Überwachung und Messung des Fortschritts der IT-Projekte im Unternehmen. Projekte können im Hinblick auf die Erreichung der Zielwerte über eine Projektbewertung sowie die Verfolgung der Änderungen am Zieldatum des Meilensteins überwacht werden.

Ein Projektkennzahlensystem ist ein Kennzahlensystem, mit dem Projekte zur Erreichung der Zielwerte überwacht werden können. Eine neue Projektbewertung kann in regelmäßigen Intervallen erzeugt werden, um das Projekt gemäß den Kennzahltypen zu überwachen, die für das Projektkennzahlensystem konfiguriert wurden. Für jeden Kennzahltyp, der ein Kriterium der Auswertung darstellt, können die aktuellen und die Zielwerte definiert werden, sowie der Kennzahltyp, der die aktuelle Leistung des Kennzahltyps in Relation zum Kennzahltyp des Zielwerts darstellt. Durchführung von Projektbewertungen im Rahmen des Projektrisikomanagements:

- Projektkennzahlensysteme müssen in den Funktionalitäten **Bewertungen und Portfolios** sowie in der Funktionalität **Klassenkonfiguration** des Moduls **Konfiguration** konfiguriert werden. Informationen hierzu finden Sie im Abschnitt *Konfigurieren von Referenz- und Bewertungsdaten, die für das Projektmanagement erforderlich sind* im Referenzhandbuch *Konfigurieren von Bewertungen und Referenzdaten in Alfabet*.
- Kennzahlen für ein Projekt und dessen untergeordnete Projekte werden auf der Ansichtsseite *Projektbewertung* des entsprechenden Projekts definiert.
- Die Projektkennzahlensysteme sind dann auf der Ansichtsseite *Bewertungshistorie*verfügbar.
- Das Zieldatum der Projektmeilensteine kann auf der Ansichtsseite *Projektverfolgung-Übersichtsbericht* verfolgt werden.

Bevor Sie beginnen können, das Risiko für das Projektportfolio zu bewerten, müssen Projekte in Alfabet erfasst und verfolgt werden, indem die Projektportfolio-Governance-Funktion im Vertriebspaket „IT Planning Advanced“ berücksichtigt wird. Meilensteine werden anhand des vollständigen Vertriebspakets „IT Planning Complete“ erfasst. Detaillierte Informationen zum Erzeugen von Projekten und Verfolgen ihrer Meilensteine in Alfabet finden Sie im Referenzhandbuch *IT-Planung - fortgeschritten*.

Kapitel 5: Compliance-Management

Die Einhaltung von Richtlinien ist entscheidend für Unternehmen, die sich mit IT-Umgebungen von Finanzinstituten und Behörden auseinandersetzen, da auch eine leichte Sicherheitsverletzung eine erhebliche Beeinträchtigung herbeiführen kann. Unternehmen müssen die Compliance für verschiedene Gesetzgebungen und Standards einschließlich beispielsweise SOX, COBIT oder DSGVO bewerten und überprüfen. Die Compliance-Management-Funktion in Alfabet bietet kohärente Unterstützung für die Definition von Compliance-Anfragen, die für eine behördliche Bewertung eines bestimmten Satzes von Objekten in der IT-Architektur gestartet werden. Die Funktion ermöglicht es Ihrem Unternehmen, die Probleme und Objekte anzugeben, die durch ein Compliance-Projekt bestimmt sind, sowie das Compliance-Projekt zu verwalten, um sicherzustellen, dass es abgeschlossen wird. Interne und externe Auditoren können die Einhaltung der Abfragestruktur und die Richtigkeit der bewerteten Objekte überprüfen.

Die Funktionalität Compliance-Management in Alfabet unterstützt die Definition von Compliance-Abfragen, die Verwaltung von Compliance-Projekten, die Bewertung von Zielobjekten im Kontext eines Compliance-Projekts sowie die Überwachung von Compliance-Projekten. Die folgenden Funktionalitäten bilden die Fähigkeit des Compliance-Managements:

- Die Funktionalität *Compliance-Konfiguration* ermöglicht die Definition der Compliance-Anfrage durch Erzeugen von Compliance-Katalogen und Compliance-Domänen. Mit dem Compliance-Katalog können Sie die Zielobjekte und die für die Bereitstellung von Informationen über die Zielobjekte verantwortlichen Anwender sowie die Gruppe von standardisierten Fragen, die die Abfrage darstellen, definieren. Jedes Compliance-Projekt wird auf der Grundlage eines Compliance-Katalogs und der geografischen oder inhaltlichen Compliance-Domäne erstellt, die das Ziel der Bewertung ist.
- Die Funktionalität *Compliance-Projekte* ermöglicht das Erzeugen, Aktivieren und Verwalten von Compliance-Projekten.
- Die Funktionalität *Compliance-Bewertungen* ermöglicht es Anwendern, Fragen zu den Zielobjekten zu beantworten, für die sie im Compliance-Projekt verantwortlich sind.

Die Compliance-Projekte in Ihrem Unternehmen können in regelmäßigen Abständen initiiert werden. Sobald ein Compliance-Projekt aktiviert wurde, erhalten die Anwender, die für die Beantwortung objektspezifischer Fragen ausgewählt wurden, eine E-Mail-Benachrichtigung und Aufgabe für ihr Compliance-Projekt.

Folgende Informationen sind verfügbar:

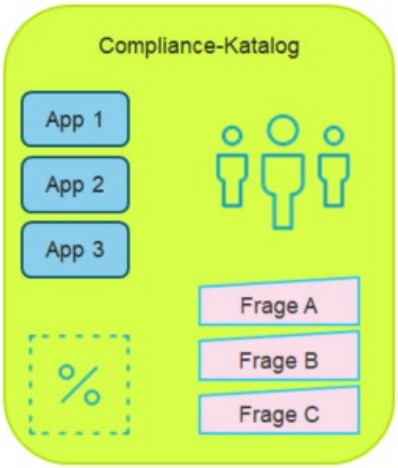
- Methodik: Verstehen des Compliance-Managements
- Voraussetzungen für Compliance-Management
- Festlegen von Compliance-Katalogen und Compliance-Domänen
- Initiieren und Verwalten von Compliance-Projekten
- Bewerten der Zielobjekte des Compliance-Projekts

Methodik: Verstehen des Compliance-Managements

Ein Compliance-Projekt stellt die Abfrage dar, die im Unternehmen gestartet werden kann, um die Einhaltung der gesetzlichen Bestimmungen von Objekten zu bewerten. Ein Compliance-Projekt könnte beispielsweise die Bewertung der SOX-Konformität für eine bestimmte Gruppe von Anwendungen im Unternehmen erreichen.

Die Compliance-Bewertung ist hochgradig konfigurierbar, basierend auf den Anforderungen Ihres Unternehmens. Jedes Compliance-Projekt basiert auf einer konfigurierten Compliance-Domäne sowie einem Compliance-Katalog. Die Compliance-Domäne gibt den gültigen Bereich an, für den das Compliance-Projekt ausgeführt werden soll. Dies könnte beispielsweise ein bestimmtes Thema oder ein geografischer Bereich sein.

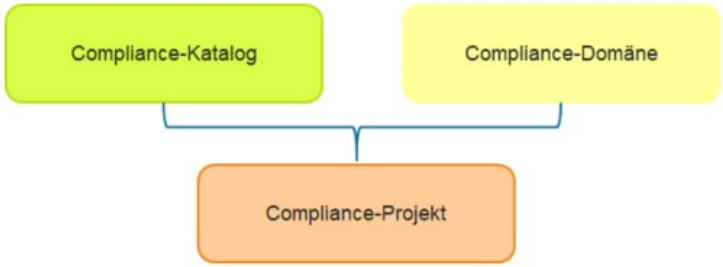
Ein Compliance-Katalog ist eine Vorlage, die für verschiedene Compliance-Projekte genutzt werden kann.



Der Compliance-Katalog bestimmt Folgendes:

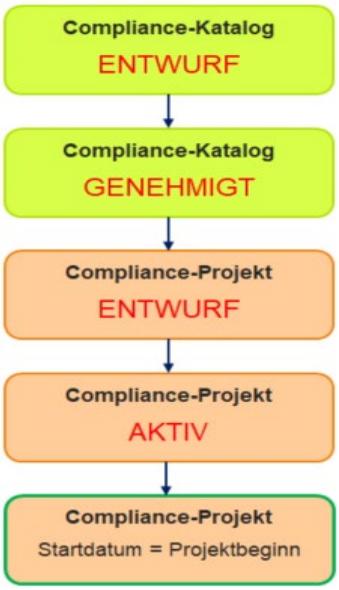
- Die Fragen zu den Objekten in der IT-Architektur. Die Fragen werden mithilfe der Compliance-Controls erfasst. Die Compliance-Controls sind hierarchisch strukturiert, wobei jede Compliance-Control der obersten Ebene eine Verzweigung im Netzwerk der Compliance-Fragen darstellt. Die Compliance-Control auf der Blattebene der Hierarchie ist die Compliance-Control, in der die Frage zum Zielobjekt definiert wird.
- Die Objekte, die Ziel der Compliance-Bewertung sind. Die von der Compliance-Bewertung vorgesehenen Objekte werden durch die Compliance-Richtlinien bestimmt, die für den Compliance-Katalog erzeugt werden. Die Compliance-Richtlinie umfasst die Abfragen, die die von der Compliance-Bewertung vorgesehenen Objekte finden.
- Die Anwender, die für die Beantwortung von Fragen zu den Objekten, die von der Compliance-Bewertung vorgesehen wurden, verantwortlich sind. Die verantwortlichen Anwender werden auch von den Compliance-Richtlinien bestimmt, die für den Compliance-Katalog erstellt wurden. Die verantwortlichen Anwender können autorisierte Anwender oder Anwender mit einer bestimmten Rolle für das Zielobjekt sein. Anwender, die keine direkte Beziehung zum Zielobjekt haben, müssen mithilfe von Abfragen gefunden werden.
- Der Kennzahltyp, der als Metrik zur Beantwortung aller Fragen in der Compliance-Bewertung verwendet wird. Ein Kennzahltyp muss zu dem Compliance-Katalog zugeordnet werden. Er wird als Metrik für alle Fragen in einem Compliance-Projekt verwendet. Beispielsweise könnte ein Indikatortyp die folgenden Werte als Antworten auf die in den Compliance-Kontrollen erfassten

Fragen zulassen: "0 – bisher keine Maßnahmen ergriffen", "1 – Compliance-Plan definiert", "2 – Plan teilweise umgesetzt", "3 – Plan vollständig umgesetzt". 4 – Nicht relevant.



Das Compliance-Projekt dient daher als Instanziierung des Compliance-Katalogs für einen bestimmten Zeitraum und Gültigkeitsbereich, die von der Compliance-Domäne bestimmt werden. Ein Compliance-Projekt, das beispielsweise auf einem Compliance-Katalog basiert, der SOX darstellt, kann die SOX-Bewertung in Q1/2020 für ein regionales Tochterunternehmen des Unternehmens sein. Ein Compliance-Projekt kann nur auf einem Compliance-Katalog basieren, wenn der Release-Status des Compliance-Katalogs als **Genehmigt** definiert ist. Es kann nur jeweils ein Compliance-Projekt für eine bestimmte Compliance-Domäne und ein bestimmtes Datum über den Status "Aktiv" verfügen.

Die im Compliance-Management implementierten Release-Status hängen von Ihrer Lösungskonfiguration ab. Jeder Compliance-Katalog und jedes Compliance-Projekt haben den Status "Genehmigt" und "Veraltet", auch wenn sie unterschiedliche Namen haben können. Im Folgenden wird ein typischer Lebenszyklus einer Compliance-Bewertung dargestellt:



- Das Attribut **Release-Status** des Compliance-Katalogs ist auf **Entwurf** gesetzt: Der Compliance-Katalog kann bei Bedarf definiert werden. Compliance-Controls können aus der Compliance-Control-Hierarchie hinzugefügt und gelöscht werden. Compliance-Richtlinien können hinzugefügt, gelöscht und bearbeitet werden. Die Attribute **Basisnutzung** und **Aktualisieren** müssen für mindestens eine Compliance-Richtlinie festgelegt werden, die der jeweiligen Compliance-Control der obersten Ebene in einem Compliance-Katalog zugeordnet ist.
- Das Attribut **Release-Status** des Compliance-Katalogs ist auf **Genehmigt** gesetzt: Die Compliance-Controls können nicht mehr hinzugefügt, gelöscht oder bearbeitet werden. Auf Basis des Compliance-Katalogs kann ein Compliance-Projekt erzeugt werden.

- Das Attribut **Release-Status** des Compliance-Projekts ist auf **Entwurf** gesetzt: Das Compliance-Projekt wird für eine ausgewählte Compliance-Domäne und für einen bestimmten Zeitraum initiiert. Compliance-Richtlinien können hinzugefügt, gelöscht und bearbeitet werden. Die Attribute **Basisnutzung** und **Aktualisieren** müssen für mindestens eine Compliance-Richtlinie festgelegt werden, die der jeweiligen Compliance-Control der obersten Ebene in einem Compliance-Katalog zugeordnet ist.
- Das Attribut **Release-Status** des Compliance-Projekts ist auf **Aktiv** gesetzt. Beachten Sie Folgendes bezüglich des Compliance-Projekts:
  - Wenn das Attribut **Release-Status** auf den genehmigten Status (**Aktiv**) gesetzt ist, wird das Compliance-Projekt aktiviert. Für Compliance-Projekte mit dem genehmigten Release-Status (**Aktiv**) ist in der Funktionalität **Compliance-Projekte** die Option **Compliance-Projekt aktivieren** verfügbar.
  - Die Compliance-Richtlinien können mit Ausnahme der Definition von **Basisnutzung** und **Aktualisieren Update** bearbeitet werden. Beachten Sie, dass diese Attribute bei einer Compliance-Richtlinie nur bearbeitet werden können, während der Release-Status eines Compliance-Projekts auf **Entwurf** gesetzt ist. Bitte beachten Sie, dass jede Compliance-Control der obersten Ebene in einem Compliance-Katalog mindestens eine Compliance-Richtlinie haben muss, die entweder als **Basisnutzung** oder als **Aktualisieren** definiert ist. Wenn dies nicht erfolgt, sind im Compliance-Projekt keine Objekte verfügbar. Dem Compliance-Projekt können jedoch keine neuen Compliance-Richtlinien hinzugefügt werden, nachdem es auf **Entwurf** gesetzt wurde.
  - Das Compliance-Projekt wird zu einem laufenden Projekt, wenn das Startdatum erreicht wird. E-Mail-Benachrichtigungen werden automatisch an verantwortliche Anwender gesendet, und Aufgaben werden für jede Compliance-Control generiert, für die sie verantwortlich sind.
  - Bitte beachten Sie die folgenden Änderungen, die an einem bereits genehmigten Compliance-Projekt vorgenommen werden können:
    - Wenn ein Compliance-Projekt genehmigt wurde, können die Compliance-Richtlinien bearbeitet werden. Dem Compliance-Projekt können jedoch keine neuen Compliance-Richtlinien hinzugefügt werden.
    - Wenn zusätzliche Objekte, die durch die Objektabfragen nicht gefunden wurden, in das Compliance Projekt aufgenommen werden müssen, ist eine Funktionalität verfügbar, die Änderungen am Compliance-Projekt ermöglicht.
  - Es kann nur jeweils ein Compliance-Projekt für eine bestimmte Compliance-Domäne über den Status "Aktiv" verfügen. Zusätzliche Compliance-Projekte können zwar für dieselbe Compliance-Domäne definiert sein, aber ihr **Release-Status** -Attribut muss auf **Entwurf** gesetzt sein, bis das vorherige Compliance-Projekt beendet ist und ihm der Release-Status **Stillgelegt** zugewiesen wird.
- Das Attribut **Release-Status** des Compliance-Projekts ist auf **Stillgelegt** gesetzt: Das Compliance-Projekt wurde abgeschlossen.
- Das Attribut **Release-Status** des Compliance-Katalogs ist auf **Stillgelegt** gesetzt: Alle laufenden Compliance-Projekte werden unwiderruflich gelöscht, und es können keine neuen Compliance-Projekte für den Compliance-Katalog erzeugt werden.

Voraussetzungen für Compliance-Management

Bevor ein Compliance-Katalog erzeugt und angegeben werden kann, müssen verschiedene Konfigurationen abgeschlossen werden.

- Das Folgende muss durch einen Lösungsentwickler im Konfigurationswerkzeug Alfabet Expand konfiguriert werden.
  - Die Objektklassen, die Ziel der Compliance-Bewertung sind. Ziel eines Compliance-Projekts können nur Objektklassen sein, die in dem XML-Objekt ***ComplianceManager*** konfiguriert wurden. Die zulässigen Objektklassen können dann im **Compliance-Richtlinien** -Editor ausgewählt werden, wenn die Compliance-Bewertung konfiguriert wird. Die folgenden Objektklassen können das Ziel einer Compliance-Bewertung sein:
    - `Application`
    - `ApplicationGroup`
    - `BusinessData`
    - `BusinessFunction`
    - `BusinessObject`
    - `BusinessProcess`
    - `Component`
    - `ComponentGroup`
    - `Demand`
    - `DemandGroup`
    - `Deployment`
    - `Device`
    - `DeviceGroup`
    - `Domain`
    - `ICTObject`
    - `ICTObjectGroup`
    - `Location`
    - `MasterPlatform`
    - `Peripheral`
    - `PeripheralGroup`
    - `Project`:<Stereotyp>
    - `MarketProduct`
    - `MarketProductGroup`
    - `StandardPlatform`
    - `Technology`
    - `TechnologyGroup`
    - `Person`
    - `Vendor`
    - `VendorProduct`
  - Die Abfragen, die zur Suche nach den Zielobjekten einer Compliance-Bewertung verwendet werden. Die Abfragen müssen in konfigurierten Berichten spezifiziert werden, deren Attribut **Kategorie** auf `Compliance` gesetzt ist. Die entsprechenden Abfragen können dann auf der Registerkarte **Objektabfragen** im **Compliance-Richtlinie** -Editor ausgewählt werden, wenn die Compliance-Bewertung konfiguriert wird.
  - Der Anwender, der für die Beantwortung einer Frage für das Zielobjekt verantwortlich ist, kann entweder der autorisierte Anwender des Zielobjekts oder ein Anwender mit einer bestimmten Rolle für das Zielobjekt sein. Wenn für die Beantwortung der Fragen zum Zielobjekt ein anderer Anwender benötigt wird, müssen Anfragen angegeben werden, um die Anwender zu finden, die für die Beantwortung der Fragen zuständig sind. Die Abfragen müssen in konfigurierten Berichten spezifiziert werden, deren Attribut **Kategorie** auf `Compliance` gesetzt ist. Die entsprechenden Abfragen können dann auf der Registerkarte **Berechtigungsregeln** im

Compliance-Richtlinie -Editor ausgewählt werden, wenn die Compliance-Bewertung konfiguriert wird.

- Sollen die Compliance-Controls in der Reihenfolge ihrer Ausführung priorisiert werden, müssen Abfragen konfiguriert werden, die die relevanten Compliance-Controls zurückgeben, die für das Compliance-Projekt beantwortet werden sollen. Die Abfragen müssen in konfigurierten Berichten spezifiziert werden, deren Attribut **Kategorie** auf `CompliancePrioritization` gesetzt ist. Die relevanten Abfragen, die für das Compliance-Projekt ausgeführt werden, können im Editor **Compliance-Projekt** im Feld **Priorisierungsrichtlinie für Compliance-Control** ausgewählt werden.
- Die Farbkodierung, die auf der *Objekte verwalten* verwendet wird, um den Abschlussstatus einer Objektbewertung zu verstehen. Dies wird auch im XML-Objekt ***ComplianceManager*** konfiguriert.
- Für die Objektklassen „Compliance-Katalog“ (`ComplianceControlSet`) und „Compliance-Projekt“ (`ComplianceControlSetInstance`) muss im XML-Objekt ***ReleaseStatusDefs*** eine Release-Status-Definition erzeugt werden. Die Release-Status-Definition gibt außerdem die Zulässigkeit des Freigabestatus an, der auf einen anderen Release-Status übertragen wird. Die im Compliance-Management implementierten Release-Status hängen von Ihrer Lösungskonfiguration ab. Jeder Compliance-Katalog und jedes Compliance-Projekt haben den Status „Genehmigt“ und „Veraltet“, auch wenn sie unterschiedliche Namen haben können. Mehr Information über das Konfigurieren von Release-Statuswerten für die Funktionalität „Compliance-Management“ finden Sie unter *Konfigurieren der Release-Status-Definitionen für Compliance-Projekte* im Referenzhandbuch *Konfigurieren von Alfabet mit Alfabet Expand*.
- Weitere Informationen zur Konfiguration des XML-Objekts ***ComplianceManager*** und der Release-Status und der Abfragen, die für die Fähigkeit „Compliance-Management“ relevant sind, finden Sie im Abschnitt *Konfigurieren der Compliance-Management-Funktionalität* im Referenzhandbuch *Konfigurieren von Alfabet mit Alfabet Expand*.

- Ein Anwender mit Zugriff auf die Funktionalität **Bewertungen und Portfolios** muss ein Kennzahlensystem konfigurieren, das den Kennzahltyp enthält, der als Metrik zur Bewertung der Zielobjekte in der Compliance-Bewertung verwendet wird. Beachten Sie, dass ein Kennzahltyp als Metrik für alle Fragen in einem Compliance-Projekt verwendet wird. Der Kennzahltyp sollte den Bereich der Werte enthalten, die als Antwort auf die Fragen ausgewählt werden können. Ein Kennzahltyp hat z. B. einen definierten Bereich wie „0 – bisher keine Maßnahmen ergriffen“, „1 – Compliance-Plan definiert“, „2 – Plan teilweise umgesetzt“, „3 – Plan vollständig umgesetzt“. 4 – nicht relevant. Beachten Sie, dass alle Fragen, die in den Compliance-Controls gestellt werden, basierend auf den Optionen beantwortbar sein müssen, die mit dem für den Compliance-Katalog definierten Kennzahltyp verbunden sind. Informationen über das Konfigurieren von Kennzahlensystemen und Kennzahltypen finden Sie im Referenzhandbuch *Konfigurieren von Bewertungen und Referenzdaten in Alfabet* unter *Konfigurieren von Bewertungen, Priorisierungsschemata und Portfolios*.

Festlegen von Compliance-Katalogen und Compliance-Domänen

Compliance-Kataloge werden in der Funktionalität *Compliance-Konfiguration* erzeugt und festgelegt: Sie können mehrere Compliance-Kataloge festlegen. Die Compliance-Controls, die für einen Compliance-Katalog definiert sind, können in einem anderen Compliance-Katalog wiederverwendet werden.

- **Erzeugen eines oder mehrerer Compliance-Kataloge für das Unternehmen**. Definieren Sie für jeden Compliance-Katalog den Kennzahltyp, durch den die Metrik festgelegt wird, mittels derer die für das Compliance-Projekt relevanten Architekturelemente bewertet werden. Beachten Sie, dass nur ein Kennzahltyp für den Compliance-Katalog implementiert werden kann. Daher müssen alle Fragen, die in den Compliance-Controls gestellt werden, basierend auf den Optionen beantwortbar sein, die mit dem für den Compliance-Katalog definierten Kennzahltyp verbunden sind. Der Compliance-Katalog wird auf der Ansichtsseite *Compliance-Kataloge* erzeugt, die in der Funktionalität *Compliance-Konfiguration* verfügbar ist.
- **Erzeugen aller Compliance-Richtlinien, die für den Compliance-Katalog relevant sind**. Sie müssen die konfigurierten Berichte angeben, die Abfragen mit festgelegten Regeln enthalten, um die Objekte zu finden, die das Ziel des Projekts sein werden, sowie die Anwender, die für die Beantwortung der Fragen zu diesen Objekten verantwortlich sind. Diese Compliance-Richtlinien werden für die Compliance-Controls zur Verfügung gestellt und müssen auf der *Compliance-Richtlinien* jeder Compliance-Control den Compliance-Controls explizit zugeordnet werden, für die sie relevant sind.
    - Für jede Compliance-Richtlinie können Sie eine oder mehrere Objektabfragen angeben, um die Objekte zu finden, die das Ziel einer Compliance-Bewertung sind. Bitte beachten Sie, dass es möglich ist, eine Warteschlange für die Compliance-Richtlinien im Kontext der *Compliance-Richtlinien* anzuzeigen, die für jede Compliance-Control verfügbar ist.

      Eine Compliance-Control, die auf die Applikationssicherheit abzielt, überprüft, ob sensible Applikationen in einer gesicherten physischen Umgebung betrieben werden. Der Compliance-Control sind zwei Compliance-Richtlinien zugeordnet. Die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** findet Applikationen, die Business-Prozesse unterstützen, die für den Vertrieb relevant sind. Die andere Compliance-Richtlinie, **Kritische Applikationen, die Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern**, findet Applikationen, die allgemein ein Fall für die IT-Sicherheit sind. Die Applikationen zur Unterstützung von Business-Prozessen können möglicherweise kritische Applikationen sein, die Zugriffssteuerung erfordern.

      Um herauszufinden, welche Applikationen, die Umsatz erzielende Business-Prozesse unterstützen, auch die Kriterien für kritische Applikationen erfüllen, die Zugriffssteuerung erfordern, müssen die Abfragen in einer Warteschlange eingereiht werden. In diesem Fall sollte zunächst die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** ausgeführt werden, und die Compliance-Richtlinie **Kritische Applikationen, die Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern** sollte anschließend als zweites Kriterium ausgeführt werden. Um dieses Abfrage-Szenario zu konfigurieren, würde das Attribut **Basisnutzung** für die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** gesetzt, und das Attribut **Aktualisieren** würde für die Compliance-Richtlinie **Kritische Applikationen, die Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern** gesetzt.

    - Für jede Compliance-Richtlinie können Sie entweder den autorisierten Anwender und/oder Anwender mit einer bestimmten Rolle angeben, um die Compliance-Fragen zu beantworten. Oder, wenn andere Anwender zur Beantwortung der Compliance-Fragen aufgefordert werden, können Sie eine oder mehrere Anfragen an die entsprechenden Anwender richten.
    - Die Compliance-Richtlinien werden dem Compliance-Katalog auf der Ansichtsseite *Compliance-Richtlinien*, die für den Compliance-Katalog zur Verfügung steht, zugeordnet.

- **Strukturieren einer Hierarchie von Compliance-Controls für den Compliance-Katalog**. Die am weitesten untergeordnete Control der jeweils untersten Hierarchieebene stellt eine Frage dar, die im Rahmen einer Abfrage gestellt werden soll.

  - Die Compliance-Controls sind hierarchisch strukturiert. Sie können eine unbegrenzte Anzahl von Compliance-Controls der obersten Ebene für den ausgewählten Compliance-Katalog erzeugen. Alle Compliance-Controls der obersten Ebene stellen eine Verzweigung im Netzwerk der Compliance-Fragen dar. Die Compliance-Controls auf der obersten Ebene der Hierarchie werden auf der Ansichtsseite *Compliance-Controls der obersten Ebene* des Compliance-Katalogs definiert.

  - Jede untergeordnete Compliance-Control wird auf der Ansichtsseite *Untergeordnete Compliance-Controls* der übergeordneten Compliance-Control definiert. Die in dieser Hierarchie am weitesten untergeordnete Compliance-Control ist die Compliance-Control, in der die Frage definiert wird. Die Frage, die in der Bewertung gestellt wird, muss im Attribut **Beschreibung** der Compliance-Control der untersten Ebene in der Hierarchie definiert werden. Beachten Sie, je niedriger die Compliance-Control in der Hierarchie der Compliance-Controls steht, desto granularer sollte die Beschreibung ausfallen. Befindet sich die Compliance-Control auf der untersten Ebene der Hierarchie der Compliance-Controls, sollte das Attribut **Beschreibung** die Frage enthalten, die für das Zielobjekt gestellt wird. Bitte beachten Sie, dass die gestellte Frage basierend auf den Optionen beantwortbar sein muss, die mit dem für den Compliance-Katalog definierten Kennzahltyp verbunden sind.

- **Zuordnen der relevanten Compliance-Richtlinien, die aus dem Compliance-Katalog definiert wurden, zu der relevanten Compliance-Control**. Alle Compliance-Richtlinien, die für den Compliance-Katalog erzeugt wurden, werden automatisch auf der *Compliance-Richtlinien* jeder Compliance-Control angezeigt, müssen jedoch bei Bedarf der entsprechenden Compliance-Control explizit zugewiesen werden. Die definierten Compliance-Richtlinien werden verwendet, um die für die Compliance-Control relevanten Zielobjekte und Anwender zu finden. Beachten Sie Folgendes:

  - Wenn die Compliance-Richtlinie für die gesamte Hierarchie der Compliance-Controls in einer Verzweigung relevant ist, sollte die Compliance-Richtlinie zu einer Compliance-Control der obersten Ebene zugeordnet werden. Das Attribut **Basisnutzung** muss für mindestens eine Compliance-Richtlinie pro relevanter Objektklasse, die der jeweiligen Compliance-Control der obersten in einem Compliance-Katalog zugeordnet ist, festgelegt werden. Wenn Compliance-Richtlinien explizit einer übergeordneten Compliance-Control zugeordnet wurden, erben die ausgewählten Compliance-Controls die Definition der Compliance-Richtlinien, es sei denn, diese Definition wird für die Compliance-Control geändert. Auf diese Weise können Sie die Zuordnung von Compliance-Richtlinien durch Hinzufügen oder Entfernen von Compliance-Richtlinien verfeinern.

  - Sie können auch eine Warteschlange für die Compliance-Richtlinien angeben, sodass Objekte, die durch eine erste Compliance-Abfrage gefunden wurden, durch eine zweite Compliance-Abfrage neu bewertet werden. Auf diese Weise können Sie angeben, dass eine Compliance-Richtlinie 1 zur Implementierung des ersten Kriteriensets zur Suche nach Zielobjekten verwendet wird. Anschließend wird eine zweite Compliance-Richtlinie zur Suche nach Objekten anhand eines zweiten Kriteriums implementiert.

    Eine Compliance-Control, die auf die Applikationssicherheit abzielt, überprüft, ob sensible Applikationen in einer gesicherten physischen Umgebung betrieben werden. Der Compliance-Control sind zwei Compliance-Richtlinien zugeordnet. Die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** findet Applikationen, die Business-Prozesse unterstützen, die für den Vertrieb relevant sind. Die andere Compliance-Richtlinie, **Kritische Applikationen, die**

Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern, findet Applikationen, die allgemein ein Fall für die IT-Sicherheit sind. Die Applikationen zur Unterstützung von Business-Prozessen können möglicherweise kritische Applikationen sein, die Zugriffssteuerung erfordern.

Um herauszufinden, welche Applikationen, die Umsatz erzielende Business-Prozesse unterstützen, auch die Kriterien für kritische Applikationen erfüllen, die Zugriffssteuerung erfordern, müssen die Abfragen in einer Warteschlange eingereiht werden. In diesem Fall sollte zunächst die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** ausgeführt werden, und die Compliance-Richtlinie **Kritische Applikationen, die Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern** sollte anschließend als zweites Kriterium ausgeführt werden. Um dieses Abfrage-Szenario zu konfigurieren, würde das Attribut **Basisnutzung** für die Compliance-Richtlinie **Applikationen, die Umsatz erzielende Prozesse unterstützen** gesetzt, und das Attribut **Aktualisieren** würde für die Compliance-Richtlinie **Kritische Applikationen, die Zugriffssteuerung und Videoüberwachungseinrichtungen erfordern** gesetzt.

  - Wenn Änderungen an den Compliance-Richtlinien vorgenommen wurden, die einer übergeordneten Compliance-Control in der Compliance-Control-Hierarchie zugeordnet sind, können Sie die ausgewählte Compliance-Control aktualisieren, sodass sie die Änderungen an den Compliance-Richtlinien erbt. Klicken Sie dazu auf der Ansichtsseite *Compliance-Richtlinien* auf die Schaltfläche **Richtlinienanpassung übernehmen**.

- **Wenn der Compliance-Katalog vollständig ist, setzen Sie den Release-Status auf "Genehmigt".** Sobald der Compliance-Katalog genehmigt wurde, können der Compliance-Katalog und die Compliance-Control-Hierarchie nicht mehr geändert werden. Bitte beachten Sie jedoch, dass die Compliance-Richtlinien für ein Compliance-Projekt mit dem **Release-Status** -Attribut auf **Entwurf** oder **Aktiv** hinzugefügt und bearbeitet werden können. Anders ausgedrückt, nachdem ein Compliance-Projekt aktiviert wurde, können die Compliance-Richtlinien im Kontext des laufenden Compliance-Projekts auf der Ansichtsseite *Compliance-Richtlinien* geändert werden.

- **Definieren der Compliance-Domänen**. Definieren Sie eine oder mehrere Compliance-Domänen, die die thematischen oder geographischen Gebiete darstellen, für die Compliance-Projekte ausgeführt werden sollen. Ein Compliance-Projekt kann für eine bestimmte Compliance-Domäne oder unabhängig von einer Compliance-Domänendefinition aktiviert werden. Die Compliance-Domäne wird auf der Ansichtsseite *Compliance-Domänen* erzeugt, die in der Funktionalität *Compliance-Konfiguration* verfügbar ist.

Initiieren und Verwalten von Compliance-Projekten

Compliance-Projekte können erzeugt werden, sobald der Compliance-Katalog genehmigt wurde. Sie können ein Compliance-Projekt in der Funktionalität *Compliance-Projekte* erzeugen, ändern, aktivieren und verwalten.

- **Erzeugen des Compliance-Projekts.** Hierzu müssen Sie die Ansichtsseite „Compliance-Katalog“ aufrufen, auf der das Projekt basiert. Ferner müssen Sie auch die Ansichtsseite „Compliance-Domäne“ aufrufen, die das Ziel des Projekts sein wird. Wird das Attribut **Release-Status** des Compliance-Projekts auf **Entwurf** gesetzt, wird das Compliance-Projekt für eine ausgewählte Compliance-Domäne und für einen bestimmten Zeitraum initiiert. Compliance-Richtlinien können hinzugefügt, gelöscht und bearbeitet werden. Ein Compliance-Projekt wird in der *Compliance-Projekte* erzeugt.

- Wenn das Attribut **Release-Status** des Compliance-Projekts auf den Status **Aktiv** gesetzt ist, wird das Compliance-Projekt aktiviert. Für Compliance-Projekte mit dem genehmigten Release-Status (**Aktiv**) ist in der Funktionalität **Compliance-Projekte** die Option **Compliance-Projekt aktivieren** verfügbar. Beachten Sie Folgendes:
  - Compliance-Richtlinien können bearbeitet werden. Dem Compliance-Projekt können jedoch keine neuen Compliance-Richtlinien hinzugefügt werden.
  - Das Compliance-Projekt wird zu einem laufenden Projekt, wenn das Startdatum erreicht wird. E-Mail-Benachrichtigungen werden automatisch an verantwortliche Anwender gesendet, und Aufgaben werden für jede Compliance-Control generiert, für die sie verantwortlich sind.
  - Bitte beachten Sie die folgenden Änderungen, die an einem bereits genehmigten Compliance-Projekt vorgenommen werden können:
    - Wenn ein Compliance-Projekt genehmigt wurde, können die Compliance-Richtlinien bearbeitet werden. Dem Compliance-Projekt können jedoch keine neuen Compliance-Richtlinien hinzugefügt werden.
    - Wenn zusätzliche Objekte, die durch die Objektabfragen nicht gefunden wurden, in das Compliance Projekt aufgenommen werden müssen, ist eine Funktionalität verfügbar, die Änderungen am Compliance-Projekt ermöglicht.
  - Es kann nur jeweils ein Compliance-Projekt für eine bestimmte Compliance-Domäne über den Status "Aktiv" verfügen. Nachfolge-Compliance-Projekte können zwar für dieselbe Compliance-Domäne definiert sein, aber sie müssen so lange den **Release-StatusEntwurf** aufweisen, bis das vorherige Compliance-Projekt beendet ist und ihm der Release-Status **Stillgelegt** zugewiesen wird.
- Wenn Compliance-Controls (die Fragen zu Zielobjekten) hinsichtlich der Reihenfolge, in der sie in einem Compliance-Projekt ausgeführt werden, priorisiert werden, können Sie zum Finden der für das Compliance-Projekt relevanten Compliance-Controls konfigurierten Berichte auswählen. So kann eine Anfrage beispielsweise festlegen, dass nur Compliance-Controls mit dem Attribut **Ebenen-ID** 1, 2 und 3 für ein Compliance-Projekt relevant sind. Sobald das erste Compliance-Projekt abgeschlossen ist, können Sie das Compliance-Projekt dann erneut starten und festlegen, dass Compliance-Controls mit dem Attribut **Ebenen-ID** 4, 5 und 6 für ein Compliance-Projekt relevant sind. Die Anfragen werden die entsprechenden Compliance-Controls zurückgeben, die im Compliance-Projekt enthalten sein sollen. Die relevanten Abfragen, die für das Compliance-Projekt ausgeführt werden, können im Editor **Compliance-Projekt** im Feld **Priorisierungsrichtlinie für Compliance-Control** ausgewählt werden.

- **Ändern der Compliance-Richtlinien**. Solange das Compliance-Projekt den Release-Status **Entwurf** aufweist, können Sie neue Compliance-Richtlinien hinzufügen oder die vorhandenen bearbeiten. Sobald eine neue Compliance-Richtlinie erzeugt wurde, muss sie den vorhandenen Compliance-Fragen manuell hinzugefügt werden. Wechseln Sie dazu zur *Compliance-Controls der obersten Ebene*, die für das Compliance-Projekt verfügbar ist. Wählen Sie zunächst die Compliance-Frage aus, auf die die neue Compliance-Richtlinie angewendet werden soll, klicken Sie dann auf die Schaltfläche **Navigieren**, und öffnen Sie die *Compliance-Richtlinien*. Klicken Sie auf die Schaltfläche **Compliance-Richtlinienanpassung**, und setzen Sie im dann angezeigten Editor ein Häkchen in der Spalte **Basisnutzung** für die Compliance-Richtlinie, die auf die Compliance-Frage angewendet werden soll.
- **Aktivieren des Compliance-Projekts**. Sobald ein Compliance-Projekt aktiviert ist, erhalten die Anwender, die für die Beantwortung zielobjektspezifischer Fragen ausgewählt wurden, eine E-

Mail-Benachrichtigung und Aufgaben für das Compliance-Projekt. Das Projekt wird am angegebenen Startdatum beginnen. Das Compliance-Projekt wird in der Funktionalität *Compliance-Projekte* aktiviert.

- **Überprüfen der vorhandenen Zielobjekte im Compliance-Projekt**. Die vorhandenen Zielobjekte werden auf der *Objekte verwalten* des Compliance-Projekts angezeigt. Sie können dem Compliance-Projekt auch zusätzliche Zielobjekte hinzufügen, die nicht durch die Compliance-Richtlinien gefunden wurden.

  Wenn keine aktive Compliance-Richtlinie für die ausgewählte Compliance-Frage verfügbar ist, werden keine Objekte für eine ausgewählte Objektklasse angezeigt. Eine aktive Compliance-Richtlinie kann auf drei Arten für die ausgewählte Compliance-Frage zur Verfügung gestellt werden:

  - Eine Compliance-Richtlinie kann von der Compliance-Control geerbt werden, die der Compliance-Control übergeordnet ist, auf der die ausgewählte Compliance-Frage basiert. Die Vererbung ist nicht möglich bei Compliance-Fragen, die auf einer Compliance-Control auf der obersten Ebene der Compliance-Control-Hierarchie basieren.
  - Wenn keine Objekte angezeigt werden, weil keine aktive Compliance-Richtlinie verfügbar ist, führen Sie einen der folgenden Schritte durch.
    - In der Funktionalität **Compliance-Projekte**: Gehen Sie zum Objektprofil des Compliance-Projekts, öffnen Sie den **Compliance-Projekt** -Editor und setzen Sie das Attribut **Release-Status** auf **Entwurf**. Gehen Sie zur *Compliance-Richtlinien* der jeweiligen Compliance-Frage, klicken Sie auf **Compliance-Richtlinienanpassung** und wählen Sie **Basisnutzung** für mindestens eine der Compliance-Richtlinien für die jeweilige Objektklasse. Dies ist nur möglich, wenn das Compliance-Projekt den Status **Entwurf** hat.

      Ob es möglich ist, den Release-Status eines Compliance-Projekts oder eines Compliance-Katalogs auf **Entwurf** zurückzusetzen, hängt von der Konfiguration des XML-Attributs `StatusTransition` im XML-Objekt ***ReleaseStatusDefs*** im Konfigurationstool Alfabet Expand ab. Informationen hierzu finden Sie unter *Konfigurieren der Release-Status-Definitionen für Compliance-Projekte* im Referenzhandbuch. *Konfigurieren von Alfabet mit Alfabet Expand*

    - In der Funktionalität **Compliance-Konfiguration**: Gehen Sie zum Objektprofil des Compliance-Katalogs, auf dem das Compliance-Projekt basiert, öffnen Sie den **Compliance-Katalog** -Editor und setzen Sie das Attribut **Release-Status** auf **Entwurf**. Gehen Sie zur *Compliance-Richtlinien* der jeweiligen Compliance-Control auf der obersten Ebene der Compliance-Control-Hierarchie, klicken Sie auf **Compliance-Richtlinienanpassung** und wählen Sie **Basisnutzung** für mindestens eine der Compliance-Richtlinien für die jeweilige Objektklasse.

- **Überprüfen der Vollständigkeit der Bewertung des Compliance-Projekts**. Allen entsprechenden Anwendern können E-Mail-Benachrichtigungen über ausstehende Compliance-Fragen geschickt werden, für die Sie zwecks Bewertung eines bestimmten Objekts verantwortlich sind. Das Compliance-Projekt kann in den folgenden Ansichten verfolgt werden, und E-Mails können gesendet werden, um Anwender daran zu erinnern, Ihre Zielobjekte zu verarbeiten:

- Auf der Ansichtsseite *Bewertungszusammenfassung* können Sie die im Compliance-Projekt zu bewertenden Objekte anzeigen, den Fortschritt der Bewertung bewerten und die verantwortlichen Anwender über deren Bewertungsaufgabe informieren.
- Auf der Ansichtsseite **Qualitätsbewertung** wird ein Tortendiagramm angezeigt, in dem die Analyse der in der Bewertung des Zielobjekts in dem Compliance-Projekt definierten Werte angezeigt wird.
- Auf der Ansichtsseite *Fertigstellungsstatus* wird ein Tortendiagramm angezeigt, das den Prozentsatz der für eine Objektklasse bereits beantworteten Fragen im ausgewählten Compliance-Projekt im Vergleich zu den noch zu beantwortenden Fragen angibt.

- **Erzeugen eines Nachfolge-Compliance-Projekts**. Das Nachfolge-Compliance-Projekt erbt alle Compliance-Controls und Compliance-Richtlinien, die für das Compliance-Projekt definiert sind, auf dem es basiert. Das Startdatum des neuen Compliance-Projekts wird automatisch auf den Tag nach dem Enddatum des ausgewählten Compliance-Projekts gelegt. Sobald das neue Compliance-Projekt erzeugt ist, können Sie die Attribute, einschließlich des Startdatums, nach Bedarf definieren. Ein Nachfolge-Compliance-Projekt wird in der Funktionalität *Compliance-Projekte* erzeugt.

Bewerten der Zielobjekte des Compliance-Projekts

Anwender, die für Compliance-Fragen zuständig sind, erhalten eine Aufgabe dazu in der Funktionalität *Eigene Aufgaben*. Mit einem Doppelklick auf die Aufgabe navigieren sie zu den Ansichten, wo gestellte Fragen zum Zielobjekt bearbeitet werden können.

Die Zielobjekte sind Bewertungen durch die verantwortlichen Anwender in der Funktionalität *Compliance-Bewertungen*. Um die Zielobjekte aufzurufen, für die ein Anwender im Compliance-Projekt verantwortlich ist, muss dieser das entsprechende Compliance-Projekt im **Compliance-Bewertungen** -Explorer doppelt anklicken: Der Anwender kann die Fragen bezüglich der Objekte auf zwei unterschiedlichen Wegen beantworten. Wizards führen den Anwender durch den Beantwortungsprozess für die relevanten Fragen:

- Auf der Ansichtsseite *Bewertung nach Objekten* können Anwender dieselbe Frage für alle relevanten Objekte in dem Compliance-Projekt Frage für Frage beantworten. Das heißt, dass Sie bei Anwendung dieses Bewertungsverfahrens eine alle Zielobjekte betreffende Frage beantworten.
- Auf der Ansichtsseite *Bewertung nach Compliance-Controls* können Anwender alle Fragen für die Objekte in dem ausgewählten Compliance-Projekt Objekt für Objekt beantworten. Das heißt, dass Sie bei Anwendung dieses Bewertungsverfahrens alle ein einzelnes Objekt betreffenden Fragen beantworten und anschließend zum nächsten Objekt übergehen können.