Liefer- und Leistungsbedingungen für Lieferanten der Union Investment Gruppe („Lieferantenhandbuch“)

Zusätzliche technische und organisatorische Vertragsbedingungen

Version 4.0
vom 16.01.2023

1. Inhalt

1 Liefer- und Leistungsbedingungen

In den vorliegenden Liefer- und Leistungsbedingungen für Lieferanten der Union Investment Gruppe werden Anforderungen zusammengefasst, die der Auftragnehmer, in Abhängigkeit von der Art und dem Umfang der von ihm zu erbringenden Leistungen, als weitere Haupt- und Nebenpflichten seiner Leistung zu berücksichtigen hat.

2 Nachhaltigkeitsanforderungen für Lieferanten der DZ BANK Gruppe

Alle Lieferanten, bzw. Dienstleister der Union Investment Gruppe sind verpflichtet die Nachhaltigkeitsanforderungen für Lieferanten der DZ BANK Gruppe anzuerkennen und einzuhalten, diese sind Voraussetzung für die Aufnahme einer Vertragsbeziehung. Ein Ausschluss dieser Verpflichtung durch andere Verträge ist ausgeschlossen.

Damit sind für den vorliegenden Auftrag die Abschnitte 2 ff „Nachhaltigkeitsanforderungen für Lieferanten der DZ BANK Gruppe“ (in der Version „DOK_UMS_015, V1.0, 21.01.2013“) der Ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

2.1 Vorwort

Eine nachhaltige Entwicklung ist für die Gesellschaften der DZ BANK Gruppe der Maßstab für eine langfristig orientierte Unternehmenspolitik, die sich nicht nur ökonomischen, sondern zugleich auch ökologischen und sozialen Herausforderungen stellt. Verantwortungsbewusst zu handeln ist für uns ein zentrales Unternehmensziel und gehört zum Selbstverständnis genossenschaftlicher Institute.

Mit dem Beitritt der DZ BANK AG zum Global Compact der Vereinten Nationen (UN) im Jahr 2008 haben wir uns außerdem zu zehn weltweit gültigen Grundsätzen verantwortlichen Handelns bekannt. Diese Grundsätze sind für uns eine wichtige Orientierung für unser Handeln (UN Global Compact[1]).

2.2 Anwendungsbereich

Im Folgenden präzisieren die Gesellschaften der DZ BANK Gruppe die Erwartungen an alle Geschäftspartner. Die Erwartungen orientieren sich u.a. an den Prinzipien des UN Global Compact[2] aus den Bereichen Menschenrechte, Arbeitsnormen, Umweltschutz und Korruptionsbekämpfung, der vom BME (Bundesverband Materialwirtschaft, Einkauf und Logistik e.V.) verabschiedeten BME-Verhaltensrichtlinie[3] „Code of Conduct“, sowie den einschlägigen Konventionen der Internationalen Arbeitsorganisation (ILO Kernarbeitsnormen[4]). Etwaige vertragliche Vereinbarungen zwischen Gesellschaften der DZ BANK Gruppe und dem Geschäftspartner werden durch diese Nachhaltigkeitserklärung nicht verdrängt.

Die Gesellschaften der DZ BANK Gruppe betrachten die Anforderungen als wesentlich für die jeweilige Geschäftsbeziehung. Bei Verstoß gegen die Nachhaltigkeitsanforderungen werden die Gesellschaften der DZ BANK Gruppe zusammen mit dem Geschäftspartner einen konkreten Maßnahmenplan erstellen. Dieser enthält auch ein Eskalationsschema, das im Extremfall bis zur Kündigung der Geschäftsbeziehung reichen kann.

---

1 United Nations Global Compact. 2015. The Ten Principles | UN Global Compact. [online] Abgerufen am (17.09.2020) <https://www.unglobalcompact.org/what-is-gc/mission/principles>

[2] United Nations Global Compact. 2015. The Ten Principles | UN Global Compact. [online] Abgerufen am (17.09.2020) https://www.unglobalcompact.org/what-is-gc/mission/principles

[3] Bundesverband Materialwirtschaft, Einkauf und Logistik e. V.. ohne Jahr. BME – Verhaltensrichtlinie. (Code of Conduct). [online] Abgerufen am (16.05.2022) https://a.storyblok.com/f/104752/x/0e28c5bcc4/bme_code_of_conduct_de_neues-logo.pdf

[4] Internationale Arbeitsorganisation. 2020. ILO Kernarbeitsnormen. Die Grundprinzipien der ILO. [online] Abgerufen am (17.09.2020) https://www.ilo.org/berlin/arbeits-und-standards/kernarbeitsnormen/lang--de/index.htm

Die Gesellschaften der DZ BANK Gruppe erwarten, dass ihre Geschäftspartner auch für die Einhaltung dieser Anforderungen durch ihre Geschäftspartner und Subunternehmer Sorge tragen, diese thematisieren und abfragen.

2.3 Nachhaltigkeitserklärung bei Aufnahme der Geschäftsbeziehung mit Geschäftspartnern

Die im Folgenden aufgeführten Erwartungen stellen Mindestanforderungen in diesem Zusammenhang dar und erheben somit keinen Anspruch auf Vollständigkeit. Die Gesellschaften der DZ BANK Gruppe erwarten, dass der Geschäftspartner die jeweils geltenden Gesetze und Regelungen sowie internationalen Standards wahrt und achtet. Strengere nationale rechtliche Maßstäbe am Sitz des Gesellschaft der DZ BANK Gruppe sind vorranging zu beachten.

2.4 Ökonomische Verantwortung

Die Gesellschaften der DZ BANK Gruppe streben eine faire und partnerschaftliche Geschäftsbeziehung mit ihren Geschäftspartnern an und übernehmen Verantwortung gegenüber den Geschäftspartnern, der Umwelt und der Gesellschaft. Wir erwarten von unseren Geschäftspartnern daher einen auf dauerhaftes und nachhaltiges Handeln ausgerichteten Geschäftsbetrieb.

2.5 Ökologische Verantwortung

Die Gesellschaften der DZ BANK Gruppe erwarten Folgendes:

Einhaltung der rechtlichen Anforderungen

Der Geschäftspartner sorgt für einen ausreichenden Umweltschutz. Hierbei erfüllt er mindestens die lokalen bzw. nationalen rechtlichen Anforderungen der Gesellschaften der DZ BANK Gruppe. Der Geschäftspartner sollte ein Verfahren zur Überprüfung der Rechtssicherheit etabliert haben.

Minimierung der Umweltbelastung

Der Geschäftspartner minimiert Umweltbelastungen und verbessert seine Umweltschutzmaßnahmen kontinuierlich. Auf Verlangen legt er den Nachweis der eingeleiteten Maßnahmen vor. Der Geschäftspartner sollte regelmäßig Vorschläge zur Verbesserung der Umweltleistung im Rahmen der Geschäftsbeziehung unterbreiten, sowie Ziele zur Reduzierung der Umweltbelastung definieren und daraus konkrete Maßnahmen ableiten.

Organisatorische Maßnahmen im Umweltmanagement

Der Geschäftspartner betreibt nachweislich ein systematisches und organisatorisch verankertes Umweltmanagement bzw. baut dieses nachweislich auf.

2.6 Soziale Verantwortung

Anerkennung und Einhaltung der Menschenrechte

Der Geschäftspartner erkennt die Menschenrechte an und hält sie ein. Dies gilt insbesondere für die Allgemeine Erklärung der Menschenrechte (AEMR)[5] der Generalversammlung der Vereinten Nationen sowie die Europäische Menschenrechtskonvention (EMRK)[6].

Keine Kinder- und Zwangsarbeit

Die Mitarbeiter des Geschäftspartners haben ein Mindestalter gemäß der Internationalen Arbeitsorganisation (ILO) Konvention 138[7]. Das Mindestalter darf weder unter dem Alter, in dem die Schulpflicht endet, noch unter 15 Jahren liegen. Zwangsarbeit einschließlich Schuldknechtschaft oder

[5] Vereinte Nationen. 1948. Resolution der Generalversammlung. 217 A (III). Allgemeine Erklärung der Menschenrechte. [online] Abgerufen am (14.02.2021) https://www.un.org/Depts/german/menschenrechte/aemr.pdf

[6] Council of Europe. 1953. Convention for the Protection of Human Rights and Fundamental Freedoms. Details of Treaty No.005. [online] Abgerufen am (14.02.2021) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

[7] Internationale Arbeitsorganisation. 1976. Übereinkommen 138. Übereinkommen über das Mindestalter für die Zulassung zur Beschäftigung, 1973. [online] Abgerufen am (14.02.2021) https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---normes/documents/normativeinstrument/wcms_c138_de.htm

unfreiwillige Häftlingsarbeit praktiziert, toleriert oder unterstützt der Geschäftspartner nicht. Strengere lokale rechtliche Maßstäbe sind vorrangig zu beachten.

Gewährleistung fairer Entlohnung und fairer Arbeitsbedingungen

Der Geschäftspartner zahlt seinen Angestellten für einen angemessenen Lebensunterhalt ausreichende und angemessene Löhne. Er hält gesetzliche Mindestlöhne ein. Der Geschäftspartner gewährleistet faire Arbeitsbedingungen für seine Mitarbeiter. Er hält nationale Gesetze und Verordnungen über Arbeitszeiten und Arbeitssicherheit sowie die Kernarbeitsnormen der Internationalen Arbeitsorganisation (ILO)[8] ein.

Vereinigungsfreiheit und Recht auf Kollektivverhandlungen

Der Geschäftspartner gesteht seinen Mitarbeitern Vereinigungsfreiheit und das Recht auf Kollektivverhandlungen zu.

Sicherstellung von Arbeitssicherheit und Gesundheitsschutz am Arbeitsplatz

Der Geschäftspartner gewährleistet die entsprechende Arbeitssicherheit für seine Mitarbeiter, um Unfällen und gesundheitlichen Beeinträchtigungen vorzubeugen. Er hält dabei mindestens die rechtlichen lokalen Anforderungen zur Arbeitssicherheit und zum Gesundheitsschutz ein. Der Geschäftspartner sorgt für Arbeitssicherheit und Gesundheitsschutz mindestens gemäß der Kernarbeitsnormen der Internationalen Arbeitsorganisation (ILO)[9], sofern gesetzliche Normen geringere Anforderungen formulieren oder diese fehlen.

Nicht-Diskriminierung

Der Geschäftspartner schließt jede Form der Diskriminierung (bspw. aufgrund Rasse, Hautfarbe, Geschlecht, Alter, Nationalität, Religionszugehörigkeit, Behinderung, sexueller Orientierung, politischer Meinung oder sozialer Herkunft) mindestens entsprechend den Benachteiligungsverboten des Allgemeinen Gleichbehandlungsgesetzes aus. Alle Mitarbeiter sind vor Belästigung am Arbeitsplatz, insbesondere sexueller Art, zu schützen.

Keine Korruption

Der Geschäftspartner akzeptiert keine Form von Korruption oder Bestechung; er lässt sich in keiner Weise darauf ein.

Der Geschäftspartner erklärt hiermit, dass er die vorstehenden Anforderungen zur Kenntnis genommen hat, umsetzt und bereit ist, die Einhaltung der Anforderungen durch die Abgabe einer Selbstauskunft (Lieferantenfragebogen der DZ BANK Gruppe) zu dokumentieren. Sollte eine Gesellschaft der DZ BANK Gruppe konkrete Bedenken im Hinblick auf die Einhaltung der Nachhaltigkeitsanforderungen durch den Geschäftspartner haben, ist dieser grundsätzlich auch bereit, der betreffenden Gesellschaft nach vorheriger Abstimmung mit ihm zu ermöglichen, die Einhaltung der Nachhaltigkeitsvereinbarung bei ihm vor Ort zu überprüfen.

Dieses Dokument ist eine Erklärung des Geschäftspartners an die Gesellschaften der DZ BANK Gruppe, mit denen der Geschäftspartner Vertragsbeziehungen hat oder haben wird. Dementsprechend tauschen die betroffenen Gesellschaften der DZ BANK Gruppe dieses unterzeichnete Dokument untereinander aus, um die Abgabe der oben genannten Erklärungen an jede dieser betroffenen Gesellschaften zu dokumentieren. Ferner haben alle Gesellschaften der DZ BANK Gruppe technischen Zugriff auf dieses unterzeichnete Dokument. Der Geschäftspartner erklärt sich damit einverstanden.

[8] Internationale Arbeitsorganisation. 2020. ILO Kernarbeitsnormen. Die Grundprinzipien der ILO. [online] Abgerufen am (14.02.2021) https://www.ilo.org/berlin/arbeits-und-standards/kernarbeitsnormen/lang--de/index.htm

[9] Internationale Arbeitsorganisation. 2020. ILO Kernarbeitsnormen. Die Grundprinzipien der ILO. [online] Abgerufen am (14.02.2021) https://www.ilo.org/berlin/arbeits-und-standards/kernarbeitsnormen/lang--de/index.htm

3 Umweltschutz und Sicherheit für Fertigung, Montage & Leistung vor Ort

3.1 Grundsätze

Wird der Auftragnehmer bei einem Unternehmen der Union Investment Gruppe vor Ort tätig, fertigt oder montiert er Werke, die bei einem Unternehmen der Union Investment Gruppe vor Ort eingesetzt oder mit denen Mitarbeiter eines Unternehmens der Union Investment Gruppe in Berührung kommen werden?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte3 ff „3 Umweltschutz und Sicherheit für Fertigung, Montage & Leistung vor Ort“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

Die Unternehmen der Union Investment Gruppe (UIG) bekennen sich im Rahmen ihrer Nachhaltigkeitspolitik zu verantwortungsvollem Handeln. Ziel dieser Anlage ist, das Verständnis für Umweltschutz und Sicherheit zu verbessern.

Grundlage des Umweltmanagements der UIG ist der „Nachhaltigkeitskodex von Union Investment“, die u.a. die folgenden Grundsätze zur Umwelt definiert (siehe auch https://unternehmen.union-investment.de/startseite-unternehmen/Nachhaltigkeit/Nachhaltigkeit-bei-Union-Investment.html):

- Ziel ist, die Umweltverträglichkeit der Produkte und Dienstleistungen der Unternehmen der UIG gemeinsam mit ihren Anlegern und Geschäftspartnern kontinuierlich zu verbessern. Die Unternehmen der UIG verfolgen daher Entwicklungen im Bereich nachhaltiger und umweltfreundlicher Finanzdienstleistungen und prüfen diese auf Anwendbarkeit für die UIG.
- Die Unternehmen der UIG nutzen die ihr zur Verfügung gestellten Ressourcen verantwortlich, effizient und sparsam. Es ist ihr Ziel, Material- und Energieverbräuche bestmöglich zu verringern sowie Emissionen und Abfallaufkommen zu minimieren.
- Bei der Beauftragung von Dienstleistungen und der Beschaffung von Waren werden auch die Umweltauswirkungen im Hinblick auf Herstellungs-, Nutzungs- und Entsorgungsphase systematisch berücksichtigt.
- Bei Investitionen und Baumaßnahmen berücksichtigen die Unternehmen der UIG im Vorfeld auch die Umweltauswirkungen und wählen – sofern aus ökonomischen Gesichtspunkten vertretbar – die umweltfreundlichere Variante. Sollten die Unternehmen der UIG diese Entscheidungen nicht unmittelbar selbst treffen können, werden sie die Entscheidungsträger in diesem Sinne beraten.
- Die Unternehmen der UIG fördern die Nutzung umweltschonender Verkehrsmittel bei Dienstreisen und Fahrten zwischen Wohnung und Arbeitsplatz. Die Unternehmen der UIG prüfen die Notwendigkeit von Dienstreisen und nutzen Alternativen wie z.B. Videokonferenzen.

Darüber hinaus wurde innerhalb der UIG ein Umweltmanagementsystem (UMS) installiert, dass seit dem 05.07.2011 nach DIN EN ISO 14001 zertifiziert ist. Der wesentliche Erfolgsfaktor eines Umweltmanagementsystems ist die kontinuierliche Verbesserung. Aus diesem Grund werden die Unternehmen der UIG regelmäßig den Erfolg all ihrer Maßnahmen zum Schutz der Umwelt selbstkritisch auf den Prüfstand stellen und, wo immer erforderlich, auch weitere Verbesserungen vornehmen.

Der Auftragnehmer wird vor Durchführung eines Auftrags seine zur Leistungserbringung tätigen Mitarbeiter in den nachfolgend aufgeführten Punkten unterweisen und dies entsprechend dokumentieren, wobei der Auftraggeber erwartet, dass der Auftragnehmer alle in diesem Dokument beschriebenen Sicherheits- und Umweltanforderungen bei der Unterweisung berücksichtigt werden. Der Auftraggeber behält sich vor, die Qualifikation der Mitarbeiter und den Nachweis zur Unterweisung in regelmäßigen Stichproben zu kontrollieren. Bei Fragen zu UI-spezifischen Themen oder zur Unterweisung eines Vorarbeiters/Multiplikators wendet der Auftragnehmer sich rechtzeitig an den Auftraggeber.

Es gelten die Bestimmungen der Brandschutzordnung, die sowohl im Intranet, als auch in den orangefarbenen Ordner „Information zum Arbeits- und Umweltschutz“ in den Teeküchen einsehbar sind.

3.2 Abfallentsorgung

Der Auftragnehmer stellt die ordnungsgemäße und umweltschonende Entsorgung aller Abfälle, die im Zusammenhang mit den beauftragten Tätigkeiten stehen, sicher. Des Weiteren gewährleistet der Auftragnehmer, dass alle nicht verbauten Materialien und Verpackungen, die er in die UIG eingeführt hat, nach ausgeführter Tätigkeit wieder mitgenommen werden bzw. ordnungsgemäß und umweltschonend der Entsorgung zugeführt werden.

Fallen im Rahmen der Leistungserbringung Abfälle in einem wesentlichen Umfang an, die als problematisch eingestuft wurden (bspw. Elektroschrott, Batterien, Gefahrstoffe), so sind die Entsorgungen in einem Abfallregister zu dokumentieren und regelmäßig an die Ansprechpartner für Abfall in der UIG zu berichten. Die Einstufung der problematischen Abfalltypen wird vor der Leistungserbringung zwischen den Vertragspartnern abgestimmt und im Abfallregister dokumentiert.

Wird dem Auftragnehmer von der UIG Material zur Verfügung gestellt, beachtet er die Abfalltrennung entsprechend den Kennzeichnungen der Abfallbehälter (Papier-, Verpackungs-, Bio- und Restmüll) in den Büro- und Küchenräumen.

3.3 Gefahrstoffmanagement

Der Auftragnehmer verzichtet auf den Einsatz von Gefahrstoffen (z.B. Reinigungsmittel, Farben, Lösungsmittel, Silikone, Lacke, Öle, Schmierstoffe, usw.) in den Räumlichkeiten der UIG. Ist der Einsatz von Gefahrstoffen unausweichlich, geschieht dies ausschließlich in Absprache mit der Fachkraft für Arbeitssicherheit am jeweiligen Standort der UIG. Vor Absprache hat der AUFRAGNEHMER den Bedarf mit dem Sicherheitsdatenblatt anzumelden.

Der Auftragnehmer stellt sicher, dass alle Mitarbeiter über die geeignete Qualifikation zum Umgang mit den aufgeführten Gefahrstoffen verfügen.

3.4 Umgang mit Ressourcen

Die zur Erbringung der Leistung eingesetzten Arbeitsmittel, Roh-, Hilfs- und Betriebsstoffe, sollten nach Möglichkeit umweltfreundlich sein und idealerweise produktspezifischen und herstellerunabhängigen Umweltstandards (bspw. FSC-Papier, Geräte mit Blauem Engel, Energieeffizienzklasse A+++, etc.) genügen.

Der Auftragnehmer geht verantwortlich mit den zur Verfügung stehenden Ressourcen um, d.h., sie werden effizient und sparsam eingesetzt.

3.5 Emissionen / Immissionen

Ist abzusehen, dass durch den Auftragnehmer im Rahmen seiner Leistungserbringung umweltrelevante Stoffe (bspw. Kühlmittel) entweichen könnten, oder die Geräusch- und Staubentwicklung die erlaubten Grenzwerte übersteigen, müssen die Verantwortlichen der UIG im Vorfeld informiert werden.

Der Auftragnehmer sollte bemüht sein, seine Leistungen möglichst umwelt- bzw. klimaneutral zur erbringen.

3.6 Verhalten im Notfall

Der Auftragnehmer und seine Mitarbeiter beachten die Vorgaben des Arbeitsschutzes und die Verfahren im Gefahrfall (z.B. Unfall oder Feuer). Die Informationen dazu erhält jeder Mitarbeiter des Auftragnehmers, der Leistungen in einem Gebäude der UIG erbringt, durch eine Unterweisung vor Beginn seiner Tätigkeit. Darüber hinaus kann er die wesentlichen Informationen dem Faltblatt „Arbeits- und Umweltschutz bei Union Investment“ entnehmen, das ihm mit der Zutrittskarte oder vom Empfang ausgehändigt wird.

Setzt der Auftragnehmer einen Notruf ab, hat er den Sicherheitsdienst bzw. den Empfang darüber zu informieren.

Bei Ertönen eines Warnsignals (Sirene, Hupe, Ansage), z.B. im Falle eines Brandes müssen die Gebäude sofort über die nächstgelegenen Rettungswege, Notfallausgänge und Nottreppenhäuser verlassen werden. Hierbei sind Personen in der Nachbarschaft zu warnen und verletzten oder behinderten Personen zu helfen. Suchen Sie die festgelegten Sammelplätze auf. **Achtung: Keine Aufzüge benutzen!**

Den Weisungen der Stockwerksbeauftragten, der Rettungskräfte und des Sicherheitsdienstes ist Folge zu leisten.

3.7 Arbeitssicherheit

Der Auftragnehmer und seine Mitarbeiter beachten die Betriebsanweisungen und Sicherheitshinweise an den Standorten der UIG.

Bei Eintritt ins Firmengebäude ohne Zutrittskarte und Mitarbeiterausweis ist ein Anmelden am Empfang erforderlich. Gleichfalls besteht eine Abmeldepflicht beim Verlassen des Gebäudes.

Das Mitbringen elektrischer Geräte und Durchführen von Veränderungen an der vorhandenen Verkabelung, sowie das Öffnen der Bodentanks sind grundsätzlich verboten. Sind zur Erbringung der Leistung dennoch elektrische Geräte nötig, dürfen diese ausschließlich an Tisch- oder Wandsteckdosen angeschlossen werden, jedoch ohne, dass dabei Stolperfallen entstehen. Die umfassende Verantwortung für einen elektrisch betriebssicheren Zustand, der im Rahmen der Leistungserbringung mitgebrachten Elektrogeräte und Zuleitungen obliegt dem Auftragnehmer. Der Auftragnehmer entscheidet im Rahmen des gesetzlichen und berufsgenossenschaftlichen Regelwerks in eigener Verantwortung über Art und Umfang der notwendigen Prüfungen und hält eine nachvollziehbare Dokumentation hinsichtlich der durchgeführten Prüfungen und deren Ergebnis vor. Gleiches gilt auch für Elektrogeräte, die der Auftragnehmer im Rahmen seines Leistungsangebotes für den Auftraggeber bereitstellt. Die Dokumentation ist auf Anfrage dem Auftragsverantwortlichen vorzulegen.

Zur Bedienung, Wartung oder Reparatur der Maschinen und Anlagen setzt der Auftragnehmer nur entsprechend eingewiesene bzw. ausgebildete/zertifizierte Mitarbeiter ein. Alle für die Auftragserfüllung verwendeten Arbeits- und Betriebsmittel müssen diesen Vorschriften entsprechen und dürfen nur in vorgeschriebener Weise benutzt werden. Soweit bei den vorgesehenen Arbeiten das Tragen persönlicher Schutzausrüstung notwendig oder vorgeschrieben ist, muss der Auftragnehmer dafür Sorge tragen, dass diese seinen Mitarbeitern zur Verfügung gestellt und bestimmungsgemäß getragen wird.

Geräte und Zuleitungen, die sicherheitsrelevante Defekte aufweisen oder außerhalb der geforderten sicherheitsrelevanten Kennwerte liegen, dürfen in den Gebäuden des Auftraggebers nicht in Gebrauch gelangen und sind unverzüglich aus den Gebäuden des Auftraggebers zu entfernen.

Sind für die Durchführung der Dienstleistung Fahrzeuge notwendig, ist dies rechtzeitig bei dem Auftraggeber anzumelden. Auf dem Gelände und in der Tiefgarage ist die Straßenverkehrsordnung einzuhalten. Das Parken ist ausschließlich auf den ausgewiesenen Plätzen erlaubt.

Muss der Auftragnehmer Leistungen an der gleichen Arbeitsstelle wie andere Fremdfirmen und/oder Mitarbeiter von Union Investment erbringen die eine gegenseitige Gefährdung oder Behinderung nicht ausschließen, so ist bereits von der Arbeitsaufnahme eine Abstimmung unter Einbeziehung des Koordinators (i.d.R. des Auftraggebers) herbeizuführen.

Der Einsatz von Subunternehmen muss an den Auftraggeber gemeldet werden. Der Auftragnehmer ist für die Einhaltung der Arbeits- und Umweltschutzbestimmungen gegenüber dem Subunternehmer alleinverantwortlich und muss dies schriftlich regeln.

Folgende Hinweise sind besonders zu beachten:

- Rauchen innerhalb des Gebäudes, der Genuss von Alkohol und sonstigen Rauschmitteln ist verboten.
- Betreten Sie nur Bereiche für die Sie eine Unterweisung erhalten haben.
- Die Arbeitsstelle ist ständig in einem ordentlichen Zustand zu halten und nach Abschluss der Arbeiten aufgeräumt zu verlassen!
- Sicherheitseinrichtungen dürfen nicht beseitigt oder unwirksam gemacht werden!
- Den Anordnungen des Sicherheitsdienstes ist Folge zu leisten!
- Für Arbeiten, die sich auf die Brandmeldeanlage auswirken können (bspw. durch Staub-, Wärme- oder Rauchentwicklung), muss ein Erlaubnisschein beim Brandschutzbeauftragten vor Aufnahme der Arbeiten beantragt werden. Mit den Arbeiten darf erst nach Erteilung und Aushändigung des Erlaubnisscheins begonnen werden.
- Jede Störung, Gefährdung und Unfälle bei der Ausführung von Arbeiten ist der Fachkraft für Arbeitssicherheit sowie dem Auftraggeber oder dem Koordinator unverzüglich zu melden. Umweltgefährdungen (bspw. Entweichen von Kühlmitteln) sind unverzüglich dem Umweltschutzbeauftragten zu melden.
- Die Ansprechpartner, Kontakte sowie Informationen zu Erste Hilfe, Sammelstellen etc. sind den Aushängen, den orangefarbenen Ordnern „Information zum Arbeit“ in den Teeküchen und Treffpunkten oder dem Flyer „Arbeits- und Umweltschutz bei Union Investment“ am Empfang zu entnehmen.

Mit Annahme bzw. Bestätigung des Auftrages bestätigt der Auftragnehmer, dass er sich an die vorgenannten Anforderungen halten wird und diese an seine für den Auftraggeber tätigen Mitarbeiter kommuniziert hat.

4 Zugangsarten und Zugangsberechtigungen

Für Auftragnehmer bestehen verschiedene Zugangsarten und Zugangsberechtigungen, die in Abhängigkeit der von ihm zu erbringenden Lieferung und Leistung durch die verantwortlichen Stellen der Union Investment Gruppe vergeben werden. Diese können den physischen Zugang zu Gebäuden umfassen, die der Union Investment als Eigentümer gehören, in denen sich die Union Investment als Mieter befindet, bis hier zu Zugangsarten, die sich als administrativer Zugriff auf das Netzwerk der Union Investment bezieht.

Art und Umfang des Zugangs und der Berechtigungen wird ausschließlich durch die verantwortliche Stelle der Union Investment im Zusammenhang mit dem für die Durchführung des jeweiligen Auftrages festgelegt. Ein Anspruch auf Gewährung eines Zugangs, welcher Art auch immer, ohne direkten Bezug zu einem Auftrag besteht nicht. Ferner darf keine der nachfolgend beschriebenen Zugangsarten für einen anderen als den im jeweiligen Auftrag beschriebenen Zweck verwendet werden.

4.1 Zutrittsberechtigungen und Zutrittskarten (Deutschland)

Werden Mitarbeiter des Auftragnehmers eigenbeweglich in den Gebäuden der Union Investment Gruppe, ausgenommen hiervon sind Besucher (diese sind über Besucherausweise abgedeckt) und Handwerker (individueller Zugang per Überwachung durch Stockwerksbeauftragten) sein?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte4 ff „Zutrittsberechtigungen und Zutrittskarten (Deutschland)“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

4.1.1 Kartenverwaltung:

Ansprechpartner für die Kartenverwaltung ist die Ausweisstelle.

Mail:	Ausweisstelle@Union-Investment.de
Telefon:	+49 69 2567 2020
Büro:	Neue Mainzer Straße 6-12, 60311 Frankfurt/Main

4.1.2 Kartenausgabe:

Für die Ausgabe einer Zugangskarte an externe Mitarbeiter/Berater bedarf es der Beantragung durch die jeweilige Abteilungsleitung bzw. einer von ihr autorisierten Stelle.

Es sind nur dann Zugangskarten für externe Mitarbeiter zu beantragen, wenn der externe Mitarbeiter auch tatsächlich über einen längeren Zeitraum in den Räumlichkeiten der UI tätig sein wird, d. h. mindestens wöchentlich Zugang benötigt.

Die ausgestellten Zugangskarten müssen persönlich direkt bei der USG_BS oder beim Sicherheitsdienst abgeholt werden. Ein Versand von Zugangskarten mittels Post/Hauspost ist nicht gestattet.

Ergänzend zur Zugangskarte erhält der externe Mitarbeiter den Flyer „Arbeits- und Umweltschutz bei Union Investment“.

Zugangskarten für externe Mitarbeiter werden nur für maximal ein Jahr freigeschaltet. Die Beantragung einer Verlängerung der Freischaltung kann per E-Mail durch den UI-Auftraggeber erfolgen.

Bei den Buchungen an Zutrittslesern wird die Kartennummer, Name, Vorname, Ort, Datum und Zeit gespeichert. Die Daten werden nach Rückgabe der Zugangskarte wieder gelöscht.

Karten von externen Mitarbeitern, die länger als 42 Tage nicht benutzt werden, werden automatisch gesperrt.

Die Zugangskarte ist eine persönliche Legitimation und darf nur vom registrierten Nutzer verwendet werden. Die Weitergabe der Zugangskarte ist untersagt, ebenso ist ein auch nur kurzzeitiges Verleihen nicht gestattet.

Bei Zuwiderhandlungen wird die Zugangskarte gesperrt und entzogen.

Alle sonstigen Kartennutzer (z.B. Handwerker, Lieferanten) erhalten die Zugangskarte sowie den Flyer „Arbeits- und Umweltschutz bei Union Investment“ direkt von der UIP-AV nach vorheriger Anmeldung durch den UI-Auftraggeber.

Die Zugangskarte wird zeitlich und räumlich befristet freigeschaltet.

Die Zugangsberechtigung wird individuell festgelegt.

Die Beantragung oder Verlängerung zeitlich befristeter Handwerkerkarten ist rechtzeitig bei UIP-AV von der zuständigen Abteilungsleitung oder einem von ihr autorisierten Mitarbeiter formlos per Email zu beantragen.

Die beantragende Abteilung hat darauf zu achten, dass die externen Mitarbeiter bzw. der Dienstleister ausreichend im Arbeits- und Umweltschutz unterwiesen sind. Siehe hierzu den Absatz „Umwelt- und Arbeitsschutzbestimmungen für Fremdfirmen in der Union Investment Gruppe (UIG)“.

4.1.3 Zugangsberechtigung Sonderräume

Änderungswünsche an der Zugangsberechtigung zu den in den Gebäuden befindlichen Sonderbereichen sind der UIP-BS in jedem Fall schriftlich per E-Mail (mittels Formular „Anforderung Zugangskarten für externe Mitarbeiter“ siehe Kapitel 4.1.2) mitzuteilen. Eine Erweiterung der räumlichen Zugangsberechtigung erfolgt nur bei Vorliegen einer schriftlichen Genehmigung durch den Verantwortlichen des entsprechenden Bereiches.

4.1.4 Kartenrückgabe

Zugangskarten werden ausschließlich an die UIP-BS zurückgegeben.

Für die termingerechte Kartenrückgabe (spätestens am Tag des Ausscheidens) ist bei externen Mitarbeitern/Beratern die jeweilige Abteilungsleitung bzw. die von ihr autorisierte Stelle verantwortlich.

Unabhängig von der Rückgabe wird bei externen Mitarbeitern die Karte im Zutrittskontrollsystem gesperrt.

Nicht zurückgegebene Karten können in Rechnung gestellt werden.

4.1.5 Kartenverlust

Kartenverluste sind vom Kartennutzer schnellstmöglich der UIP-BS telefonisch oder per E-Mail mitzuteilen. Auf Basis einer solchen Verlustmeldung erfolgt seitens der UIP-BS umgehend die Sperrung der Zugangsberechtigungen für alle Gebäude.

Wenn die Karte unwiederbringlich verloren erscheint, bekommt der externe Mitarbeiter eine neue Karte. Die neue Kartennummer wird dem Service Desk mitgeteilt, um die verlorene Karte aus der Druckerverwaltung zu löschen. In Frankfurt wird außerdem der Caterer informiert, um das Payment-Guthaben entsprechend zu übertragen und die verlorenen Karte in deren System zu sperren.

Um verloren gegangene Zugangskarten wieder zu erhalten, ist auf der Kartenrückseite eine Finderadresse vermerkt.

Verlorengegangene Karten können in Rechnung gestellt werden.

4.1.6 Vergessene Karten

Bei vergessenen Karten kann dem entsprechenden Mitarbeiter eine Ersatzkarte von der UIP-BS ausgestellt werden. An den Empfängen MTP, WINX und NM14 ist ein Kontingent von Ersatzkarten hinterlegt. Zur Ausgabe der Ersatzkarte wird die Ausweisstelle informiert.

Die Karte ist spätestens am nächsten Arbeitstag wieder zurückzugeben.

Frankfurt:

Bei Vergessen der Zugangskarte werden an den Empfängen der Frankfurter Standorte Name, Datum, Uhrzeit und Abteilungszugehörigkeit dokumentiert.

4.1.7 Defekte Zugangskarten

Defekte Zugangskarten werden von der Union Investment Privatfonds GmbH – Business Services (UIP-BS) „Ausweisstelle“ ausgetauscht.

4.1.8 Tragepflicht von Besucher- oder Mitarbeiterausweisen

Die Verpflichtung, einen Mitarbeiterausweis der UI zu tragen, gilt für alle Personen, die sich in den Gebäuden der Union Investment Gruppe aufhalten.

Externen Mitarbeitern muss ein Ausweis durch den Beauftragenden zur Verfügung gestellt werden. Zusammen mit dem Ausweis wird eine Plastikhülle zur Befestigung mit Halteclip und auf Wunsch einem Gewebetrageband ausgehändigt

Der Ausweis ist gut sichtbar zu tragen.

Die Ausweise für externe Mitarbeiter, die über einen längeren Zeitraum als einen Monat ihren ständigen Arbeitsplatz in den Bürogebäuden der Union Investment Gruppe haben, tragen grundsätzlich ein Farb-Lichtbild des externen Mitarbeiters, dessen Namen, das Logo von Union Investment und das Verbundlogo. Außerdem enthalten sie den Zusatz „Extern“ unter dem Namenszug.

Die Ausweise von Personen, die sich lediglich im Rahmen der Durchführung einer Dienstleistung (z.B. Handwerker, etc.) in den Bürogebäuden der Union Investment Gruppe aufhalten oder Personen, die als „Externe“ über einen kürzeren Zeitraum als einen Monat ihren ständigen Arbeitsplatz in den Bürogebäuden der UIG haben, sind anstatt mit dem Lichtbild mit dem Aufdruck „Extern“ beziehungsweise „Handwerker“ und fortlaufender Nummerierung versehen.

Am Standort Frankfurt am Main versteht sich der Mitarbeiter-Ausweis als rein passives Instrument zur optischen Kontrolle der Aufenthaltsberechtigung von Personen in den Gebäuden der Union Investment Gruppe.

Bei Austritt des Mitarbeiters ist dieser zur unaufgeforderten Rückgabe seines Mitarbeiterausweises verpflichtet. Der Ausweis ist an den Beauftragenden oder direkt an die Allgemeine Verwaltung (UIP-BS) zurückgegeben.

Zurückgegebene Ausweise werden nach dem Vier-Augen-Prinzip von UIP-BS vernichtet und die Vernichtung dokumentiert. Ebenso werden alle nicht mehr benötigten Bilddateien die UIP-BS vorliegen, nachweislich gelöscht.

4.1.9 Verlust

Bei Verlust des Ausweises ist der Mitarbeiter verpflichtet, diesen Verlust unverzüglich und

unaufgefordert UIP-BS mitzuteilen. Es wird kurzfristig ein neuer Ausweis erstellt.

4.1.10 Erstellung eines Mitarbeiterausweises

Für die Erstellung der Ausweise ist UIP-BS zuständig. Für die Produktion bedient sie sich eines externen Dienstleisters. Dieser Dienstleister ist gesondert den Vorschriften der EU-DSGVO verpflichtet.

Die Lichtbilder von den externen Mitarbeitern stellt die beauftragende Abteilung der UIP-BS zur Verfügung.

Für die Richtigkeit der Schreibweise des Namens und der evtl. Zusatzbezeichnung „Extern“ ist der Mitarbeiter bzw. der Beauftragende des externen Mitarbeiters verantwortlich.

UIP-BS verwaltet die Bilddateien und kann diese nur mit einer schriftlichen Einverständniserklärung (E-Mail) des jeweiligen Mitarbeiters an Dritte herausgeben. Die Weitergabe von Bilddateien zu dienstlichen Zwecken unterliegt den datenschutzrechtlichen Bestimmungen als besondere Ausprägung von personenbezogenen Daten.

Nach Rückgabe der Mitarbeiterausweise an UIP-BS werden vom Dienstleister alle Bilddateien der entsprechenden Personen nach den Vorschriften der EU-DSGVO von seinen Datenträgern (Festplatte, CD-ROM, etc.) gelöscht, bzw. nicht reproduzierbar vernichtet.

4.2 Netzwerkzugang, Zugriff auf IT-Systeme und Plattformen

Erhält bzw. verfügt der Auftragnehmer bzw. seine Mitarbeiter über einen Zugang (z.B. auch per VPN-/RAS) zum Netzwerk der Union Investment Gruppe?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 4.2 ff „Netzwerkzugang, Zugriff auf IT-Systeme und Plattformen“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

4.2.1 Zweckbindung der Nutzung

Erhält der Auftragnehmer Zugang auf die IT-Infrastruktur oder auch durch Dritte für die Union Investment betriebene Systeme z.B. in Form von Zugang auf das Intranet der Union Investment Gruppe, deren Ablagesystems oder einer Kollaborationsplattform, o.ä. so ist die Nutzung immer an einen betrieblichen Zweck des zwischen dem Arbeitgeber des Nutzers als Auftragnehmer der UIT oder einer anderen Gesellschaft der Union Investment Gruppe (kurz UIG) gebunden und beschränkt. Dies gilt unabhängig davon ob der Zugriff unmittelbar oder mittelbar (i.S. als Subunternehmer eines Lieferanten bzw. Dienstleiters) erfolgt.

Nutzer im Sinne dieser Vereinbarung kann nur eine natürliche Person als Erfüllungsgehilfe des Auftragnehmers der beauftragenden Gesellschaft der Union Investment Gruppe sein. Die beauftragende Gesellschaft der Union Investment Gruppe gestattet dem Nutzer nach Maßgabe der Beauftragung die gewährten Zugriffe ausschließlich im Rahmen seiner Leistungserbringung für die Union Investment Gruppe zu nutzen. Das eingeräumte Nutzungsrecht ist nicht übertragbar. Der Nutzer handelt dabei im Namen seines Arbeitgebers, d.h. des Auftragnehmers der beauftragenden Gesellschaft der Union Investment Gruppe.

Eine Nutzung der Zugriffsmöglichkeiten für Dritte, insbesondere Wettbewerber der Union Investment Gruppe ist dem Nutzer untersagt. Auch die Weitergabe der Zugriffsmöglichkeiten oder Zugriffsgewährung an Dritte sind dem Nutzer verboten.

4.2.2 Zeitliche Beschränkung

Die Zugriffsgewährung wird dem Nutzer immer nur zeitlich begrenzt, maximal für die Dauer und den inhaltlichen Rahmen des jeweiligen Vertrags (Auftrag/Beauftragung) zwischen dem Auftraggeber und dem Auftragnehmer, eingeräumt. Die Zugriffsgewährung für den Nutzer endet automatisch, ohne dass es einer Kündigung bedarf, wenn der jeweilige Vertrag zwischen dem Auftragnehmer und dem Auftraggeber endet.

Die beauftragende Gesellschaft der Union Investment Gruppe kann die Zugriffsgewährung jederzeit nach eigenem Ermessen einschränken oder einstellen.

4.2.3 Beauskunftung über Nutzungsumfang

Auf Anforderung erteilt der Auftragnehmer dem Auftraggeber schriftlich Auskunft über die Art und den Umfang seiner Nutzung der gewährten Zugriffsmöglichkeit. Die beauftragende Gesellschaft der Union Investment Gruppe ist berechtigt, Einsicht in die mit dem Zugriff erzeugten Daten zu nehmen.

Die im Zuge der Nutzung zur Anzeige gebrachten, oder bezogenen Inhalte (z.B. Informationen aus dem Intranet) der Gesellschaften der Union Investment Gruppe sind für den Nutzer vertraulich. Der Nutzer wird die so erhaltenen Informationen vertraulich halten. Es gelten des Weiteren die sonstigen vertraglich vereinbarten Regelungen zur Vertraulichkeit und Geheimhaltung.

5 Agentur- und Marketingleistungen

Die Marken der Union Investment Gruppe sind zentrale Elemente der immateriellen Wertschöpfung unseres Unternehmens. Marken sind Vorstellungsbilder in den Köpfen interner und externer Zielgruppen. Starke Marken beeinflussen den Unternehmensumsatz und Aktienkurs ebenso wie die Aktienkaufbereitschaft und den Return to Shareholder positiv. Sie geben Orientierung, prägen die Präferenzen und schaffen Vertrauen, was gerade in Zeiten wachsender Komplexität zunehmend an Bedeutung gewinnt.

Entsprechende Aufwände und zeitliche Disposition aus der Berücksichtigung und Anwendung der Vorgaben des Auftraggebers hinsichtlich der Elemente der Markenführung hat der Auftragnehmer für seine Leistungserbringung einzukalkulieren und einzuplanen.

5.1 Agenturleistungen, Kontakter, Produktioner

Wird der Auftragnehmer auch Steuerungsleistungen im Zusammenhang von Marketingproduktionen erbringen und hierbei im Namen und Auftrag des Auftraggebers Leistungen bei Drittunternehmen beauftragen und steuern?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 5.1 ff „Agenturleistungen, Kontakter, Produktioner“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

5.2 Beauftragung von Drittunternehmen

Sofern Lieferantenleistungen von Drittunternehmen erforderlich sind, holt der Auftragnehmer abhängig von den nachfolgend aufgeführten Betragsgrößen Angebote und Kostenvoranschläge von Drittunternehmen ein, legt sie dem Auftraggeber vor und spricht Empfehlungen aus, wobei der Auftraggeber jeweils auch eigene Drittunternehmen benennen kann. Diese Regelung gilt nicht bei Folgeleistungen eines bereits zwischen den Parteien einvernehmlich ausgewählten Lieferanten.

Betragsgrößen:

- bis EUR 5.000,- inkl. Umsatzsteuer: mind. 1 schriftliches Angebot
- bis EUR 50.000,- inkl. Umsatzsteuer: mind. 2 schriftliche Angebote
- ab EUR 50.001,- inkl. Umsatzsteuer: mind. 3 schriftliche Angebote

Der Auftrag an einem Drittunternehmen darf der Auftragnehmer erst nach schriftlicher Genehmigung der Bestellung durch den Auftraggeber erfolgen. Der Auftragnehmer vergibt nach schriftlicher Genehmigung des Auftraggebers die Aufträge an Drittunternehmen im eigenen Namen und für eigene Rechnung.

5.3 Freigabe von Produktionsaufträgen

Der Auftragnehmer koordiniert und überwacht die Auftragsabwicklung hinsichtlich Qualität, Kosten und Terminen. Im Rahmen der Steuerung hat der Auftragnehmer für die Auftragserteilung an Drittunternehmen folgende Schritte zu durchlaufen:

- Der Auftragnehmer zeigt dem Auftraggeber jeweils die Produktionsreife der Leistungen des Drittunternehmens schriftlich oder in Textform (z.B. per E-Mail) an.
- Der Auftraggeber erklärt dem Auftragnehmer schriftlich oder in Textform (z.B. per E-Mail) die Zustimmung oder Ablehnung zu den von dem Auftragnehmer gemachten Vorschlägen zur Realisierung.
- Die Freigabe zur Produktion bzw. Umsetzung des gesamten Vorhabens oder auch Teilschritten erfolgt schriftlich durch den Auftraggeber.
- Der Auftragnehmer stellt sicher, dass die Umsetzung bzw. Produktion entsprechend den freigegebenen Unterlagen erfolgt.

- Im Falle einer Ablehnung durch den Auftraggeber ist der Auftragnehmer verpflichtet, unverzüglich neue Vorschläge zu unterbreiten.
- Der Auftragnehmer wird den Auftraggeber fortlaufend über den Stand der Umsetzung des Vorhabens informieren.

Er koordiniert die Auftragsabwicklung auch hinsichtlich der Rechnungs- und Zahlungsabwicklung sowie der Rechnungskontrolle. Bei Reklamation beim Drittunternehmen wird er unverzüglich die Bearbeitung und Erledigung vornehmen.

5.4 Abwicklung von Zahlungen und Abgaben

Die Zahlung an das Drittunternehmen erfolgt unter Inanspruchnahme von Skonto, wenn Skontoregelungen zwischen dem Auftragnehmer und dem Drittunternehmen vereinbart wurden. Bei der Weiterberechnung an den Auftraggeber werden den Rechnungen des Lieferanten Kopien der Originalrechnungen der Drittunternehmen beigefügt. Dem Auftragnehmer gewährte Skonti sind explizit auszuweisen. Im Einzelfall hat der Auftragnehmer hierbei in Vorleistung zu treten, wenn ansonsten das Skonto für den Auftraggeber gefährdet würde.

Der Auftragnehmer wird mit der Überwachung des Steuerabzugs ausländischer Drittunternehmen gem. § 50a Absatz 4 EStG sowie die Klärung zollrechtlicher Fragen beauftragt. Der Auftraggeber ist entsprechend zu informieren. Abgaben, die nachträglich entstehen, werden von dem Auftragnehmer übernommen.

5.5 Erstellung von Materialien, Redaktionsarbeiten, Pflege von Social Media-Kanälen

Fertigt der Auftragnehmer Materialien oder Inhalte für Union Investment an, oder tritt für und im Namen von Union Investment in der Öffentlichkeit auf?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 5.5 ff „Erstellung von Materialien, Redaktionsarbeiten, Pflege von Social Media-Kanälen“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

5.6 Corporate Design-Richtlinien im Zusammenhang mit der Markenführung

Eine erfolgreiche Markenführung muss sowohl nach außen als auch nach innen funktionieren. Ebenso wie die Mitarbeiter der Union Investment Gruppe müssen auch die durch den Auftragnehmer der Union Investment produzierten Materialien (einschl. digitalem Inhalt) diesem Anspruch genügen. Um einen hohen Wiedererkennungswert von Union Investment über alle Segmente und Medien hinweg zu garantieren, ist der konsequente und konsistente Einsatz der wesensprägenden Merkmale unerlässlich.

Union Investment pflegt hierzu Corporate Design-Richtlinien, die konsequent anzuwenden sind. Diese Richtlinien können vom Auftraggeber hier abgerufen werden: https://cd-neu.union-investment.de/Startseite.html. Dazu zählen unter anderem die folgenden Basiselemente: Logo, Farbklang, Markenform, die Schrift Frutiger Neue in allen Umsetzungen (Ersatzschrift Arial für Office-Anwendungen), Bildstil, Iconstil, Animationsstil, Soundlogo.

5.7 Unternehmenssprache

Unsere Unternehmenssprache folgt den sechs Regeln unserer Marke. Sie helfen beim Schreiben von Texten, beim Präsentieren, wenn wir eine Rede verfassen oder ein Gespräch führen:

- Vorausschauend:
  - Wir sprechen über vorausschauendes Denken und Handeln und sagen, was der Kunde davon hat
  - Wir reden über Trends und Entwicklungen und bieten eine Vorschau
  - Wir berichten, was wir als Nächstes tun und was unsere nächsten Schritte sind
- Professionell:
  - Wir betonen unsere Erfahrung und Qualität im Fondsgeschäft

- Wir bringen unsere Fachmeinung zum Ausdruck, die wir klar begründen
- Wir vermitteln ein Gefühl von Sicherheit und Vertrauen
- Wir versprechen nichts, was nicht garantiert ist
- Wir übertreiben nicht, bleiben realistisch und beschönigen nichts

- Partnerschaftlich:
  - Wir betonen Partnerschaft, stellen Fragen und ermuntern zum Dialog
  - Wir geben Tipps und zeigen Lösungen auf
  - Wir sprechen eine menschliche Sprache

- Solide:
  - Wir betonen unser solides Handeln
  - Wir verwenden keine Modewörter und erfinden keine Kunstwörter
  - Wir sprechen eine bodenständige Sprache
  - Wir meiden die Umgangssprache und verzichten auf hausinterne Ausdrücke

- Entlastend:
  - Wir sprechen eine klare, leicht verständlich Sprache
  - Wir formulieren einfach, kurze Sätze
  - Wir sprechen deutsch
  - Wir meiden Fremdwörter und Fachbegriffe
  - Wir verwenden keine Wortkürzel und verzichten auf Abkürzungen

- Erkennbar:
  - Wir achten auf das Erscheinungsbild unserer Marke
  - Wir schreiben den Namen unseres Unternehmens korrekt. Wir sind niemals die „Union“, sondern immer „Union Investment“
  - Wir schreiben die Namen unserer Fonds, Lösungen und Leistungen korrekt

Weitere Details zur Unternehmenssprache von Union Investment Segment Privatkunden, Tipps zur Texterstellung und Formulierungsvorschläge finden Sie im Handbuch „So spricht Union Investment“. Dies können Sie über Ihren Ansprechpartner oder die E-Mail-Adresse sprache@union-investment.de anfordern.

6 Lieferung und Leistungen in der Informationstechnologie

6.1 Entwicklung und Anpassung von Software und Softwarekomponenten

Wird durch den Auftragnehmer eine Anwendung auf Grundlage eigener Prozesse und Verwendung eigener vom Lieferanten definierten und/oder betriebenen Tools und Umgebungen entwickelt oder weiterentwickelt?

Handelt es sich bei der Entwicklung oder Weiterentwicklung der Anwendung aus Sicht des Auftraggebers um eine Eigenentwicklung oder ist diese als Individualentwicklung in seinem Architekturmanagement-Tool (LeanIX) kategorisiert?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 6.1 ff „Entwicklung und Anpassung von Software und Softwarekomponenten“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

6.1.1 Anforderungen an die Realisierung

Nachfolgend werden die Mindestanforderungen beschrieben, die durch den Auftragnehmer bei der Entwicklung einer Software für den Auftraggeber zu erfüllen sind.

6.1.2 Allgemeine Anforderungen an die Prozesse

Für alle Aktivitäten der Realisierung gelten folgende allgemeine Vorgaben:

- Die Abläufe sind zu definieren und zu dokumentieren.
- Verantwortlichkeiten für die einzelnen Arbeitsschritte sind definiert.
- Es existiert ein definierter Anforderungsmanagementprozess. Die Umsetzung von neuen Anforderungen wird ausschließlich über den Anforderungsmanagementprozess initiiert.
- Das Ergebnis der Realisierung sind deploybare Softwareartefakte, die mit der Anforderung zu verknüpfen sind, bspw. durch Verweis in das Sourcecode- bzw. Artefakt-Repository.
- Es ist zu gewährleisten, dass der entwickelte Sourcecode im Zugriff des Auftraggebers ist. Alternativ sind entsprechende Vereinbarungen zu treffen (bspw. Escrow-Agreement).
- Nur durch den Auftraggeber abgenommene Softwareartefakte dürfen in die Produktionsumgebung überführt werden. Hier gelten die Regelungen aus dem „Release und Deployment Management“.

6.1.3 Anforderungen an die Softwareentwicklung/Programmierung

Die Realisierung von Anwendungen – unabhängig ob Neuentwicklung oder Anpassung – erfolgt stets in einer hierfür geeigneten Entwicklungsumgebung. Es ist sicherzustellen, dass die Entwicklungsaktivitäten keine Auswirkung auf die Produktionsumgebung haben, so dass bspw. Tests der Entwicklung keine Produktionsdaten beinhalten und bspw. Performancetests die Produktionsumgebung nicht beeinflussen.
Dem Auftraggeber ist der Zugriff auf die Entwicklungsumgebung zu gewähren.
Zusätzlich gelten folgende Vorgaben:

- Es existieren anwendungsspezifische Vorgaben an die Programmierung, bspw. in Form eines Entwicklerhandbuchs oder Entwicklungs-Guidelines. Die Programmiervorgaben sind vom Auftragnehmer regelmäßig auf Aktualität zu prüfen.
- In die Programmiervorgaben sind Aspekte aufzunehmen, die die Lesbarkeit und die Wartbarkeit des Codes erhöhen und gewährleisten, bspw.
- Verweis auf gängige Marktstandards
- Verweis auf Best Practice, wie bspw. Clean-Code
- Vorgaben für Verzeichnisstrukturen und Dateinamen der Artefakte, die im Rahmen der Programmierung erstellt werden
- Namenskonventionen

- Vorgaben für die Strukturierung von Code und den Einsatz von Kontrollstrukturen (Bedingungen, Schleifen), sofern sie von anerkannten Best Practice Standards abweichen
- Vorgaben für Kommentierung und Dokumentation innerhalb des Codes
- Zur Gewährleistung eines einheitlichen Coding-Stils ist innerhalb der IDE eine geeignete Konfiguration bereitzustellen und nach Möglichkeit die Nutzung entsprechender Werkzeuge bspw. zur statischen Codeanalyse vorzusehen.
- Die eingesetzten Werkzeuge (IDE, Sourcecode-Verwaltung, Build-Tools, Deployment-Tools) sind definiert und deren Nutzung ist beschrieben.
- Sämtliche entwickelte Quellcodes und zugehörige Standardkonfigurationen sind grundsätzlich in einem Sourcecode-Repository mit Versionsverwaltung und Rechtesteuerung abzulegen. Deploybare Artefakte werden ausschließlich über den Quellcode aus dem Sourcecode-Repository gebaut.
- Ein Rechtekonzept steuert den Zugriff auf den Sourcecode.

6.1.4 Sichere Anwendungsentwicklung

Bereits während des Auswahlprozesses bzw. Vertragsanbahnungsphase erhält der potentielle Auftragnehmer von dem Auftraggeber eine Beschreibung der Vorgaben für die „sichere Anwendungsentwicklung“ gemäß *UIT Security-Standard Anwendungsentwicklung* in Form eines von Auftraggeber separat zur Verfügung gestellten und zwischen den Vertragsparteien abgestimmten Anforderungskatalogs (Checkliste).

6.1.5 Anwendungsspezifische Vorgaben

Neben den Aspekten der Lesbarkeit/ Wartbarkeit des Codes und der Sicherheit enthalten die Programmierrichtlinien Vorgaben, die sich auf das Design der Anwendung beziehen und auf die Erfüllung übergeordneter nicht-funktionaler Anforderungen (wie Performance, Sicherheit, Nachvollziehbarkeit) abzielen. Beispielhaft könnten folgende Aspekte in die Richtlinien aufgenommen werden:

- Performance: Hinweise auf besonders ressourcenintensive bzw. -schonende Berechnungs- oder Datenzugriffsverfahren
- Nutzung von Abstraktionsschichten beim Zugriff auf Datenbanken
- Nachvollziehbarkeit: Nutzung von Logging-Mechanismen
- Festlegung von fachlichen Konstanten und Look-Up-Mechanismen
- Festlegung des Fehlerhandlings
- Entkopplung von Komponenten
- Validierung und Bereinigung von User-Input

6.1.6 Anforderungen an die Softwarebereitstellung

Über die allgemeinen Vorgaben hinaus gelten bei der Softwarebereitstellung zusätzlich folgende Vorgaben:

- Die eingesetzten Werkzeuge sind definiert und beschrieben.
- Es gelten die Vorgaben aus dem „Release und Deployment Management“ bezüglich des Rollouts von neuen Anwendungen oder Artefakten.
- Es kann jederzeit eine lauffähige und produktionsidentische Version der Anwendung erzeugt werden, sobald die Anwendung in Betrieb genommen wurde.

6.2 Test-, Release- und Deployment Management

Werden durch den Auftragnehmer, in der Rolle als Hersteller, Dienstleister oder Provider, Anpassungen technischer und/oder fachlicher Art vorgenommen oder bereitgestellt, die wesentlichen Änderungen an

produktiven IT-Systemen darstellen? Es gilt die regulatorischen Vorgaben MaRisk, InvMaRisk, BAIT und für rechnungsrelevante Systeme in der GoBS und FAIT1 zu beachten.

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 6.2 ff „Test-, Release- und Deployment Management“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

6.2.1 Test-Management

In den regulatorischen Vorgaben MaRisk, InvMaRisk, BAIT, KAIT (Herausgeber: BAFIN) und für rechnungsrelevante Systeme in der GoBS (Herausgeber: Bundesministerium der Finanzen) und FAIT1 (Herausgeber: Institut der Wirtschaftsprüfer, IDW) wird übereinstimmend gefordert, dass die Produktivnahme von wesentlichen Änderungen an IT-Systemen nur nach vorheriger Freigabe durch den fachlich und technisch Verantwortlichen erfolgen darf. Änderungen können dabei technischer und/oder fachlicher Art sein. Ziel des Testens ist es, durch eine entsprechende Qualitätssicherung bei der Entwicklung und Wartung von Hard- und Softwaresystemen, eine angemessene Qualität zu erreichen und diese über den gesamten Lebenszyklus aufrechtzuerhalten. Es ist zu prüfen, ob die an das System gestellten Anforderungen erfüllt sind. Schäden, die durch nicht erkannte Fehler entstehen, sollen von der Union Investment Gruppe abgewendet bzw. minimiert werden.

Die Grundlagen für die Tests sind die vom Auftraggeber definierten funktionalen und nicht-funktionalen Anforderungen (insbesondere die Sicherheitsanforderungen), die im Pflichtenheft, im Fachkonzept, in User-Stories oder Vergleichbarem enthalten sind, sowie die sicherheitsbezogenen Programmierrichtlinien. Die Testtiefe wird in erster Linie von einem zu erwartenden Schaden bei einem nicht ausgeführten oder unvollständigen Test bestimmt.

Für Tests sind von Auftragnehmer abhängig vom Änderungsumfang Testkonzepte zu erstellen und dem Auftraggeber zur Prüfung der Eignung vorab der Testdurchführung vorzulegen.

6.2.1.1 Testdurchführung

Im Rahmen von Änderungen an IT-Systemen der Union IT-Service GmbH sind verschiedene Teststufen zu durchlaufen:

- Entwicklertest/ Modultest: Dieser Test ist durch die verantwortlichen Entwickler, bzw. das Entwicklerteam umzusetzen.
- Technischer Funktionstest/ Systemtest: Mit diesen Tests wird sichergestellt, dass die Funktionalität der Anforderungen aus technischer Sicht sichergestellt ist.
- Fachlicher Funktionstest/ Abnahmetest: Vollumfänglicher Test aller Anforderungen, d.h. der funktionalen und nicht-funktionalen Anforderungen, inklusive der sicherheitsbezogenen Anforderungen. Hierbei handelt es sich um den User Acceptance Test (UAT) durch den Auftraggeber oder einem vom Auftraggeber beauftragten Dritten.
- Betriebsübernahmetest: Es gibt zwei Arten von Betriebsübernahmetests:
    - Für Anforderungen, die sich nicht im Rahmen der vorherigen Teststufen in einer nicht-produktiven Umgebung testen lassen, ist ein Betriebsübernahmetest in Produktion durchzuführen.
    - Im Rahmen der Umsetzung von Changes ist die erfolgreiche Installation zu testen.

6.2.1.2 Testdokumentation und Aufbewahrung

Durchgeführte Tests sind in einer Testdokumentation zu dokumentieren. Die Testdokumentation ist revisionssicher aufzubewahren:

- Für GoBS-/ GoBD relevante Systeme, d.h. Systeme, die steuerrelevante Daten verarbeiten, endet die Aufbewahrungsfrist 10 Kalenderjahre nach Abschaltung des Systems.
- Für alle sonstigen Systeme gilt eine Aufbewahrungsfrist von 10 Kalenderjahren, beginnend ab dem Folgejahr.

Die Dokumentation ist dem Auftraggeber auf Anfrage zu jederzeit bereitzustellen.

Die Dokumentation ist in der Form zu erstellen, dass sie sachkundige Dritte nachvollziehen können.

6.2.1.3 Anforderungen an die Durchführung von Abnahmetests

Um sicherzustellen, dass der Abnahmetests Aussagen in Bezug auf den späteren produktiven Betrieb zulässt, sind folgende Maßnahmen umzusetzen. Der Auftragnehmer hat in Bezug auf diese Maßnahmen eine seinem Auftrag entsprechende Mitwirkungspflicht.

- Der Umfang des Abnahmetests ist dem Umfang der Änderung angemessen zu gestalten.
- Entwicklungen und Anpassungen durch Entwickler finden ausschließlich in den dafür vorgesehenen Entwicklungs- oder Testumgebungen statt. Ein Paket darf nur in einer Abnahmeumgebung bereitgestellt werden, wenn es zuvor in den Testumgebungen einen Entwicklertest und technischen Test durchlaufen hat.
- Die für den Abnahmetest verwendete Abnahmeumgebung ist in Bezug auf die Änderung in wesentlichen Aspekten zur Produktionsumgebung vergleichbar zu gestalten.

  Zu den zu beachtenden Aspekten gehören:

  - Die Hardware- und Softwareausstattung auf allen Systemkomponenten inklusive der Clients.
  - Die Testdatenmenge.
  - Die Schnittstellen.
  - Die Rahmenbedingungen, wie Einbettung in die UIT-Netzinfrastruktur.
- Werden nach Beginn das Abnahmetest größere Änderungen an der Abnahmeumgebung vorgenommen, ist zu bewerten, ob dies Auswirkungen auf die Aussagekraft des bisherigen Tests hat. Falls dem so ist, ist der Test insgesamt oder in Teilen zu verwerfen und erneut durchzuführen.

6.2.1.4 Fachliche Abnahme

Die fachliche Abnahme umfasst die Anforderungen des fachlichen Funktionstests / Abnahmetest und dessen Verantwortlichkeiten unter Einbeziehung des BISO (Business Information Security Officer, Data Owner) des Auftraggebers und der von ihm bereitgestellten bzw. begutachteten Daten, um hierdurch in einem produktionsnahen Umfeld bzw. Zustand die Abnahmetests durchführen zu können. Hierzu obliegt es dem Auftragnehmer den Auftraggeber in dem für die Durchführung dieser Tests erforderlichem Maße personell, sowie mittels erforderlicher Systemzugriffe, Daten und Anleitung etc. zu unterstützen.

Für den Fall, dass Auftragnehmer den Abnahmetest organisatorisch verantwortet, gilt: der Auftragnehmer hat den Auftraggeber mit den nach Art, Komplexität und Umfang hinreichend erscheinendem Vorlauf über die bevorstehenden Tests zu informieren.

6.2.2 Release- und Deployment-Management

Ziel des Release- und Deployment-Managements ist es, negative Auswirkungen von Releases auf die Services des Auftraggebers zu vermeiden. Das Release- und Deployment-Management fokussiert auf die Planung und die Durchführung von Änderungen an Services und sogen. Managed Services. Es stellt im Zusammenwirken mit dem in Kap. 7.3 beschriebenen Change-Management sicher, dass alle operativ vorgenommenen Änderungen an Services (Systeme, Software, Hardware, Daten etc.) für alle von einer Änderung betroffenen Stakeholder nachvollziehbar sind.

6.2.2.1 Grundsätze

Aus den genannten Zielen lassen sich die Anforderungen an den Auftragnehmer, bzw. folgenden Grundsätze, die Auftragnehmer zu beachten hat, ableiten:

- Auftragnehmer muss eigene, dem Auftraggeber in Anbetracht der von Auftragnehmer zu erbringende Leistung angemessene Release- und Deployment-Management sowie Change Management Prozesse betreiben.
- Auftragnehmer benennt einen Releasemanager, der als Ansprechpartner für Auftraggeber fungiert. Die Releasemanager beider Seiten tauschen sich nach Bedarf über die jeweiligen Releaseaktivitäten ab und ergreifen bei Konflikten oder Qualitätsproblemen entsprechende Maßnahmen.
- Die Release- und Deployment-Management des Auftraggebers macht die Vorgaben bezüglich der von Auftragnehmer vorzulegenden Releaseplanung und Dokumentationsumfang, Durchführung des eigentlichen Rollouts und Deployments von neuen oder geänderten Services nebst evtl. zugrundeliegenden Änderungen an Applikationen, Software oder Hardware.
- Auftragnehmer hat sicherzustellen, dass Deployments nur auf Basis etablierter Branchenstandards durchgeführt werden.
- Vom Auftragnehmer ist mindestens eine Jahresplanung vorzulegen, zu der der Auftragnehmer unaufgeforderte eine monatliche Fortschreibung zur Verfügung stellt. Diese Planungen sind mit dem Auftraggeber abzustimmen.
- Der Auftragnehmer stellt sicher, dass für die Umsetzung von Anforderungen des Auftraggebers ein geplantes Vorgehen angewendet wird. Umsetzungen sind in einer Releaseplanung festzuhalten und dem Auftraggeber zu kommunizieren. Ein Release ist so zusammenzustellen, wie es auch später in der Zielumgebung ausgebracht werden soll. Für das Deployment des Releases ist in der Produktionsumgebung ein erprobtes, standardisiertes Verfahren einzusetzen. Ist das nicht möglich, so ist das Deployment des Release in der Abnahmeumgebung bereits Teil des Abnahmetests und es ist identisch zu dem für die Zielumgebung geplanten Verfahren umzusetzen (vergl. Kap. 6.2.1.3 Anforderungen an die Durchführung von Abnahmetests).
- Auftragnehmer dürfen nur getestete und vom Auftraggeber abgenommene Komponenten (vergl. Kap. Test-Management) in der Zielumgebung ausrollen. Auftragnehmer müssen dabei ihre bei Auftraggeber auszuführen beabsichtigten Rollouts zügig, sicher und benutzergerecht durchführen. Die mit dem Rollout verbundenen Aktivitäten müssen hierzu von Auftragnehmer hinsichtlich ihrer Abhängigkeiten, Auswirkungen und zeitlichem Verlauf geplant und überwacht werden. Der Auftragnehmer hat sich auf Grundlage dieser Planung mit dem Auftraggeber abzustimmen und ihn über die Fortschritte informiert zu halten. Die von Auftragnehmer zu erstellende Rollout-Planung muss auch teilweise oder vollständige Rollbacks für den Fall vorsehen, dass nicht alle Changes erfolgreich ausgerollt werden können.
- Der Auftragnehmer stellt nach Vorgabe von FAIT 1 und FAIT 5 bei der Übergabe von Entwicklung in den Betrieb die Funktionstrennung sicher.
- Der Auftragnehmer hat die Bereitstellung von Software in der Art durchzuführen, dass eine Deployment-Automation angewendet werden kann. Auftragnehmer, deren erbrachtes Leistungsspektrum die Betreuung und den Betrieb umfasst, automatisieren Deployments soweit möglich.
- Für den Auftragnehmer, dessen für den Auftraggeber erbrachtes Leistungsspektrum die Betreuung und Betrieb von Applikationen und/oder Infrastruktur umfasst gilt:
    - Ist das Deployment Management ein Teil seiner Leistungsverpflichtung. Hiernach erbringt der Auftragnehmer Changes, d.h. Veränderungen die nach ihrer Art und Umfang die (Change-Typen) Infrastruktur, Hardware, Software, Daten und Wartung vorgenannter Komponenten das Deployment Management als Bindeglied zwischen dem Rollout und dem Change Management wirken. Das Deployment Management ist zudem auch für solche Changes anzuwenden, die nicht Teil des vorgenannten Release

Managements sind, wenn durch den Change die vorgenannten Elemente (Change-Typen) betroffen sind.

- Der Auftragnehmer erstellt gemeinsam mit dem Auftraggeber ein Handbuch, in dem sie das gemeinsame Releasemanagement festschreiben. Das Handbuch regelt mindestens Art und Form des gemeinsamen Releaseplans, eingesetzte Tools und Verfahren, Rollen und Ansprechpartner. Alternativ zur Benennung eines Ansprechpartners stellt der Auftragnehmer die Informationen zum Releaseplan und zu den eingesetzten Verfahren transparent, aktuell und automatisch aufrufbar zur Verfügung.
- Der Auftragnehmer setzt Verfahren auf, mit denen es möglich ist, bei Bedarf eine Wiederherstellung frühere Stände – sowohl Software als auch Daten – eines Systems wiederherstellen zu können. Die Aufbewahrung der alten Stände richtet sich nach gesetzlichen und regulatorischen Vorgaben, insbesondere GoBD, und dem Zweck der Applikationen.

- Der Auftragnehmer setzt für sämtliche Tools für Deployments und Software-Paket-Repository und weitere Funktionen bevorzugt Tools nach Vorgabe des Auftraggebers oder Tools des Auftraggebers ein. In Abstimmung zwischen Auftragnehmer und Auftraggeber kann hiervon abgewichen werden.

6.2.2.2 Minutenfahrpläne/ Detailablaufpläne für umfangreiche Deployments

Der Auftraggeber setzt für umfangreiche Deployments sogenannte Minutenfahrpläne/ Detailablaufpläne ein. In dem Ablaufplan wird für alle Beteiligten, dies sind neben Auftraggeber und Auftragnehmer teils weitere Unternehmen, eine zeitliche Planung aufgestellt, aus der hervorgeht, wann wer welche Aktivitäten durchführt. Im Rahmen dieser Planung werden Beteiligte und deren Kontaktdaten zentral erfasst.

Der Auftragnehmer hat die Erreichbarkeit der in dem Ablaufplan benannten Ansprechpartner zu den vereinbarten Zeiten sicherzustellen.

Ablaufpläne sind zusammen mit dem Change (siehe Kapitel 7.3 Change-Management) abzulegen und zu archivieren. Ablaufpläne, die im Rahmen eines Deployments ausschließlich bei dem Auftragnehmer vorliegen, sind dem Auftraggeber auf Anfrage bereitzustellen.

7 Serviceprozesse und Steuerungsaufgaben

Die Leistungserbringung für die Unternehmen der Union Investment Gruppe hat insbesondere im Kontext von Leistungen der Informationstechnologie, aber auch anderer Leistungen, die in wesentlichen Bestandteilen oder nur mittelbar auf das Funktionieren von lieferantenseitig bereitgestellten Komponenten der Informationstechnologie (z.B. IT-Plattform, Portal, Datenverarbeitung und/oder -bevorratung) angewiesen sind, mindestens über folgende IT-Service Management Prozesse ausreichenden Umfangs und Güte zu beinhalten.

Dabei kann unterschieden werden, ob der Auftragnehmer über eine von dem Auftraggeber als ausreichend erachtetes eigenes Governance-Modell und systemunterstützte Service Prozesse verfügt, die an die Systeme des Auftraggebers per Schnittstellenkopplung verbunden werden, oder ob der Auftragnehmer zwar über die organisatorischen Voraussetzungen verfügt, gleichwohl aber für die Systemunterstützung die Systeme des Auftraggebers nutzt bzw. zu nutzen hat. In letztgenanntem Fall akzeptiert der Auftragnehmer zugleich die nachfolgenden Prozesse und wird diese entsprechend beachten und anwenden.

7.1 Incident- und ServiceRequest-Management Prozess

Ist der Auftragnehmer bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 7.1 ff „Incident- und ServiceRequest-Management Prozess“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

Ziel des Incident Management Prozesses ist die schnellstmögliche Wiederherstellung der vereinbarten Service-Leistung. Dieses Ziel ist essentiell, da durch Störungen die vereinbarte Service-Leistung, die im Fokus des Service Managements liegt, direkt negativ beeinflusst wird, bzw. Anwender und Nutzer der entsprechenden Leistung und/oder Komponente beeinträchtigt sind.

Ziel des ServiceRequest-Management Prozesses ist es, die Anfrage eines Nutzers nach einer standardisierten und Serviceleistung oder einer Information in Bezug auf einen existierenden IT-Services schnell und effizient zu realisieren.

Incident-Management und ServiceRequest-Management sind in ihrer operativen Ausprägung derart ähnlich, dass nachfolgend die Bezeichnung Vorgang bzw. Incident synonym auch für den ServiceRequest verwendet wird.

Das Incident- / ServiceRequest-Management (nachfolgend aus als „IncM“ abgekürzt) umfasst Erfassung, Klassifizierung, Durchführung von Analyse und Diagnose, Service Wiederherstellung, Incident verfolgen, überwachen und abschließen, Dokumentationsgüte prüfen und Erstellung von Incidents Reports. Sofern für die von Auftragnehmer zu erbringende Leistung einschlägig, ist dies vom Auftraggeber zu erbringen. Die nachfolgenden Handlungen sind vertragliche Nebenpflichten des Auftragnehmers, insofern er z.B. keine eigene Systemunterstützung für die IT-Service Prozesse verfügt, und erbringt der Auftragnehmer auf den von Auftraggeber bereitgestellten Systemen.

7.1.1 Verantwortlichkeiten und Rollen im Incident-/ServiceRequest-Management

Der Auftragnehmer interagiert im Incident Management des Auftraggebers mit folgenden Rolleninhabern entsprechend der zugehörigen Verantwortlichkeiten.

- Process Owner - Incident Management
- Incident Manager
- Major Incident Koordinator
- First Level Operator
- Second Level Operator

Hierbei hat der Auftragnehmer zumindest die Rolle als First Level Operator wahrzunehmen, als auch in seiner eigenen Organisation entsprechende Verantwortlichkeiten für eine ebenegerechte Interaktion mit dem Auftraggeber implementiert haben. Darüberhinausgehende Rollenwahrnehmung kann der Auftraggeber vertraglich verlangen.

7.1.2 Vorgangserfassung

In diesem Prozess werden Incident Records (für Störungen) erstellt und durch den Auftragnehmer überprüft, ob der Anwender support-berechtigt ist. Falls die Prüfung negativ ausfällt, wird die Anfrage erfasst und mit dem Abschlussgrund „Kein Supportanspruch“ im System geschlossen.

Wird vom Anwender mitgeteilt, dass eine gemeldete Störung bereits beseitigt ist, wird dies entsprechend im dazugehörigen Incident Record dokumentiert.

Wünscht der Anwender Informationen zum Status der Bearbeitung eines bestehenden Incident Records, werden ihm diese Informationen durch den Auftragnehmer bereitgestellt und von ihm entsprechend im Incident Record dokumentiert.

Werden vom Anwender zusätzliche Informationen zu einem bereits erfassten Incident Record geliefert, werden diese Informationen von dem Auftragnehmer im dazugehörigen Incident Record dokumentiert.

7.1.3 Vorgangsklassifizierung

In diesem Schritt wird der erfasste Incident Request durch den Auftragnehmer kategorisiert, d.h. bei der Störung wird auf Basis der vom Anwender gemeldeten Symptome versucht, die Störung einer bestimmten Fehlerklasse zuzuordnen.

Für den Vorfall werden die Auswirkung und Dringlichkeit festgelegt; aus diesen ergibt sich die Priorität, mit der der Vorfall bearbeitet werden soll.

Für Störungen wird der Auftragnehmer dann bestimmen, ob ein Major Incident vorliegt. Major Incidents sind Störungen der Priorität 1, deren (tatsächliche oder potentielle) Wiederherstellungsdauer die vertraglich vereinbarte Wiederherstellungsdauer um 100% überschreitet. In der Konsequenz wird der weitere Incident Management Prozess für Major Incidents mit einem höheren Ressourceneinsatz durchgeführt; außerdem werden entsprechende Informationen an den Auftraggeber gegeben.

Der Auftragnehmer wird in der Knowledge DB prüfen, ob bereits ein entsprechender Fehler bekannt ist. Über die Knowledge DB werden dokumentierte Problems (Unknown Errors), Known Errors, Interims Solutions und Solutions mit ggf. bereits bekannten Workarounds zur Verfügung gestellt.

Kann keine sofortige Service Wiederherstellung herbeigeführt werden, wird der Incident Record an eine Instanz weitergeleitet, die das benötigte Fachwissen zur Herbeiführung der Service Wiederherstellung besitzt - in der Regel die nächst höhere Instanz der Rollenmatrix.

7.1.4 Analyse und Diagnose des Vorgangs

Der Auftragnehmer wird den im Incident Record beschriebene Sachverhalt analysieren und einen Service Wiederherstellungsansatz suchen. Falls eins der folgenden Kriterien erfüllt ist, ist durch den Auftragnehmer ein Problemticket aus dem Incident Prozess heraus zu erzeugen:

- Major Incident und Prio 1 Incident Pflichtfeld: Referenzierung zum Problem Ticket für den Zustandswechsel gelöst
- Mehrfache Störung/ Wiederkehrende Störungen: sind bereits mehrere gleichartige Störungen bekannt, bei denen festgestellt wurde bzw. die vermuten lassen, dass sie auf einer gemeinsamen Ursache basieren, ist ein Problem/Known Error zu eröffnen. (Incident-Vorlage beinhaltet zwingend eine Referenzierung auf ein Problemticket)
- Wenn die Gefahr besteht, dass der Incident wieder auftreten kann: Ist der Bearbeiter im Incident Management der Ansicht, dass eine erstmals auftretende Störung unter Umständen zukünftig wieder auftreten kann, ist ein Problem zu eröffnen
- Handover als Known Error: Für Störungen, für die im Rahmen der Störungsanalyse bereits die Ursache ermittelt wurde, wird ein Problem vorgeschlagen, es besteht die Möglichkeit

innerhalb des Problem Tickets die Ursache aus Sicht des IncM zu dokumentieren/vorzuschlagen. Der Ergebnisse der Ursachenanalyse sind im Problem Management zu verifizieren und bei positiven Ergebnis wird das Problem in den Zustand Known Error gebracht.

Weiter wird der Vorfall auf eine mögliche Security Relevanz untersucht und bei positivem Befund gekennzeichnet. Zur Prüfung einer möglichen Relevanz ist das bereitgestellte Template „Klassifikation von Security Incidents“ zu nutzen.

Bei Bedarf wird weitere Unterstützung angefordert, wenn mit dem vorhandenen Fachwissen und den verfügbaren Mitteln kein Behebungsansatz gefunden werden kann.

7.1.5 Service wiederherstellen

In diesem SUB-Prozess wird die im Incident Record beschriebene Serviceeinschränkung durch das Umsetzen des gefundenen Workarounds, (Interim-) Solution behoben. Stellt sich heraus, dass die umgesetzte (Interim-) Solution/ Workaround nicht die beabsichtigte Wirkung zeigt, wird erneut eine Analyse und Diagnose eingeleitet.

Wird mit der Umsetzung der gefundenen (Interim-) Solution/ Workaround die erwünschte Wirkung erzielt, wird dies im dazugehörigen Incident Record dokumentiert.

7.1.6 Vorgang abschließen

In diesem SUB-Prozess erfolgt eine Überprüfung der Dokumentation im Incident Record durch den Incident Management 1st/2nd Level Operator, in Sonderfällen auch externe Mitarbeiter mit einem äquivalenten Funktionsprofil, auf Klassifizierung, Vollständigkeit, Lesbarkeit und Wiederholbarkeit, die bei Bedarf angepasst wird (vgl. hierzu DocQ-1, Dokumentation „Kriterien zur Dokumentationsgüte Messung“). Zusätzlich wird die Abschlusskategorie für spätere Auswertungszwecke vergeben beziehungsweise angepasst und der Ticketstatus auf „Abgeschlossen“ gesetzt sofern keine Mängel festgestellt wurden.

Sofern es sich um eine Prio1 oder Prio1 Major Incident handelte, wird technisch sichergestellt das hierzu ein korrespondierendes Problemticket erstellt und mit dem Incident Ticket verlinkt wurde.

Wird in Rahmen des Incident Prozesses ein Verfahren entwickelt das nach Einschätzung des Incident Operators ggf. mehrfach angewendet werden kann (z.B. Workaround oder [Interim] Solution) so ist zu prüfen, sofern nicht bereits verlinkt, ob hierzu ein bestehendes Problem existiert. Dieses ist zu aktualisieren, andernfalls ist ein entsprechendes Problem Ticket dem Problem Management vorzuschlagen (Tool gestützte Funktion (Handover Incident Management => Problem Management).

7.1.7 Vorgangsverfolgung und überwachen

Es obliegt dem Auftragnehmer regelmäßig zu überprüfen, ob die vereinbarten Service Level bei der Bearbeitung der Incident Records eingehalten werden. Hierzu:

- Sind durch die Incident 1st/2nd Level Incident Management Operatoren täglich die ihrer Service Unit zugewiesenen Ticktes auf drohende Service Level Verletzungen zu prüfen und entsprechende Abhilfe zu schaffen
- Wird automatisch eine Maileskalation an die zugehörige Support Unit durch das Incident Management System generiert falls für Prio 1 Tickets bereits 70% der Servicewiederherstellungszeit verbraucht wurden.

Ziel ist die Voraussetzungen für eine zeitgerechte Bearbeitung der Incident Records zu ermöglichen.

7.1.8 Dokumentationsgüte prüfen

Durch die Incident Manager des Auftraggebers werden monatlich die Güte der Dokumentation der abgeschlossenen Incidents überprüft. Dazu werden Stichproben aus den Incidents des Berichtszeitraums gezogen und anhand der definierten Gütekriterien: Klassifizierung, Vollständigkeit, Lesbarkeit und Wiederholbarkeit überprüft. Sollten Incidents Tickets den geforderten Gütekriterien nicht entsprechen, so wird das Ticket mit dem Flag „Überarbeitung notwendig“ gekennzeichnet und an die betroffene Support Unit (u.a. den zu Erfassung und Bearbeitung verantwortlichen Auftragnehmer)

zur Nachbesserung zurückgegeben. Ein auf diese Weise durch den Auftragnehmer nachzubessernden Incident Record ist dann Gegenstand der nächsten turnusmäßigen Überprüfung.

7.1.9 Incident Kategorien und Aktivitätenvorlage - Nutzung prüfen

Der Auftraggeber wird in regelmäßigen Abständen die Nutzungshäufigkeit der Kategorien/ Aktivitätenvorlagen bezogen auf einen Betrachtungszeitraum anhand definierter Kriterien überprüfen. Sollten die definierten Kriterien nicht mehr zutreffen, so wird der Auftraggeber deren weitere Nutzung mit dem Auftragnehmer abstimmen. Zur Unterstützung der Überprüfung ermittelt der Auftragnehmer die in seinem Verantwortungsbereich bearbeiteten Records und liefert auf Aufforderung folgende Angaben:

- Tatsächliche Nutzung
- Nutzung trotz vorhandenem Standardservices
- Ermittlung von Häufungspunkten
- Kriterien für die Anlage und Dokumentation
- Vollständigkeit/ Wiederholbarkeit von Aktivitätenvorlagen
- Lesbarkeit Aktivitätenvorlagen

Auf Basis dieser regelmäßigen Überprüfung wird der Auftragnehmer einen Bericht erzeugen, der geeignet sein muss, sowohl in das Incident Reporting Eingang zu finden als auch einen KVP zu begründen.

7.2 Problem-Management

Ist der Auftragnehmer bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?

Falls dies der Fall ist, ist für den vorliegenden Auftrag der Abschnitte „3Problem-Management“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

Der Problem Management Prozess ist Teil des IT-Services Managements des Auftraggebers und richtet sich an den Vorgaben der ISO/IEC 20000-1:2011 aus.

Die Ziele des Problem Managements sind die Vermeidung des Wiederauftretens von Störungen und die Minimierung der Auswirkungen nicht vermeidbarer Störungen. Das Problem-Management umfasst dabei die Annahme, Analyse (Problem Control), Erarbeitung von Lösungen zur Beseitigung (Error Control) und den Abschluss. Weiterhin gehören Problem-Review und -Tracking, sowie Proaktives Problem-Management zu den Tätigkeiten innerhalb des Prozesses.

7.2.1 Verantwortlichkeiten und Rollen im Problem-Management

Der Auftragnehmer interagiert im Problem Management-Prozess des Auftraggebers mit folgenden Rolleninhabern entsprechend der zugehörigen Verantwortlichkeiten.

- Problem Expert
- Problem Manager
- Process Owner Problem Management

Hierbei hat der Auftragnehmer zumindest die Rolle als Problem Expert wahrzunehmen als auch in seiner eigenen Organisation entsprechende Verantwortlichkeiten für eine ebenegerechte Interaktion mit dem Auftraggeber implementiert haben. Darüberhinausgehende Rollenwahrnehmung kann der Auftraggeber vertraglich verlangen.

7.2.2 Vorgangserfassung

Bei der Vorgangserfassung werden sogenannte Problem-Records für potentielle oder tatsächlich aufgetretene Störungshäufungen eröffnet.

Ist die Ursache für die Störungen nicht bekannt, wird der Problem Record zudem als Unknown Error kategorisiert.

Das erkannte Problem wird priorisiert und es erfolgt eine Zuweisung des Problem Records an eine Bearbeitungsgruppe, die über das notwendige Fachwissen zur Analyse des Problems verfügt.

Treten Problems im Verantwortungsbereich des Auftragnehmers oder im Zusammenhang mit der von ihm erbrachten Leistung auf, so wird er als Bearbeitungsgruppe oder Teil einer Bearbeitungsgruppe adressiert.

7.2.3 Analyse (Problem Control) durchführen

Die verantwortliche Bearbeitungsgruppe wird eine Analyse des zugewiesenen Problems vornehmen, um die Ursache für das Problem zu ermitteln. Sollten die Voraussetzungen für die Ursachenanalyse nicht gegeben sein, obliegt es der Bearbeitungsgruppe diese in erforderlicherer Art und Umfang anzufordern.

Kann die Ursache für ein Problem bekannt, so handelt es sich nicht mehr um ein Problem, sondern um einen Known Error (bekannter Fehler). Der Record bzw. die Einträge in der Known Error-Datenbank sind von der Bearbeitergruppe entsprechend fortzuschreiben.

7.2.4 Erarbeitung von Lösungen (Error Control)

Kann die Ursache für ein festgestelltes Problem in der Analyse ermittelt werden, werden Lösungen - Solutions - erarbeitet und bewertet, die der Beseitigung der Ursache des Problems oder der Minderung der negativen Auswirkungen des Problems dienen.

Die Umsetzung der geeignetsten Lösung wird von der Bearbeitungsgruppe veranlasst und die Wirksamkeit überprüft. Bei der Entscheidung zur Anwendung einer geeigneten Lösung sind auch die Aspekte der Wirtschaftlichkeit zu berücksichtigen. Wird eine Lösung ausgewählt und zeigt die erwartete Wirksamkeit, handelt es sich um eine Final Solution. Wird die gewünschte Wirksamkeit nicht erreicht, erfolgt eine erneute Lösungssuche. Die Bearbeitungsgruppe bleibt für den Vorgang weiterhin verantwortlich.

Wird eine Lösung, die eine Ursache nachhaltig beseitigen würde nicht umgesetzt, handelt es sich um eine Interims Solution. In diesem Fall wird ein freigegebener Workaround dauerhaft angewendet.

7.2.5 Problem abschließen

Zum Abschluss eines bearbeiteten Problems wird die Dokumentation des Problem Records auf Vollständigkeit, Nachvollziehbarkeit und Korrektheit überprüft. Der Status des Problem Records wird danach auf „abgeschlossen“ geändert. Es obliegt der Bearbeitungsgruppe eine hinsichtlich Art und Umfang angemessene Qualität der Dokumentation Sorge zu tragen, damit der Problem Manager des Auftraggebers den Statuswechsel auf „abgeschlossen“ durchführen kann.

Folgende Informationen müssen im Problem Record vorhanden und für UIT verständlich und nachvollziehbar sein:

a. aussagekräftiger Titel
b. treffende Kurzbeschreibung
c. Beschreibung der Ursache für die aufgetretenen Störungen
d. Beschreibung der Lösung
e. Beschreibung des Workarounds, sofern vorhanden

7.2.6 Problem Review und Tracking durchführen

Der Fortschritt der Bearbeitung von Problem Records wird durch den Auftraggeber regelmäßig überprüft. Durch die Bearbeitungsgruppe sind angemessene Maßnahmen zu ergreifen, um die

Bearbeitung der Problem Records voranzubringen. Der Prozess Owner Problem Management und jeweiligen Problem Managern des Auftraggebers können darüber hinaus weitere Maßnahmen zur Bearbeitung durch die Bearbeitungsgruppe initiieren.

7.2.7 Proaktives Problem Management durchführen

Der Auftragnehmer soll als Teil seiner Leistungserbringung den Prozess Owner Problem Management und jeweiligen Problem Managern des Auftraggebers bei der Verfügbarkeitsanalyse durch die Bereitstellung angeforderter Daten und Informationen unterstützen. Sind für das Auftreten und den Verlauf von Incidents Trends erkennbar, wird die Eröffnung eines Problem Records geprüft und ggf. initiiert.

Gleichwohl wird der Auftragnehmer für die von ihm erbrachten Leistungen eigene Prozesse betreiben und Maßnahmen ergreifen, um proaktiv das Auftreten von Incidents zu vermeiden.

7.2.8 Vorgabedokumente / Nachweisdokumente

Alle in dem Prozess benötigten und verwendeten Dokumente werden in Vorgabe- und Nachweisdokumente eingestuft.

Vorgabedokumente sind qualitätsrelevante Dokumente, die Vorgaben (Anweisungen) hinsichtlich der Durchführung bestimmter Tätigkeiten oder Verfahren beinhalten. Hierzu zählen z.B. Richtlinien, Verfahrensanweisungen, Leitfäden, leere Formulare (Vorlagen) etc.

Nachweisdokumente sind qualitätsrelevante Dokumente, die Nachweise (Aufzeichnungen) hinsichtlich der Durchführung bestimmter Tätigkeiten und/oder Verfahren beinhalten. Hierzu zählen z.B. ausgefüllte und abgestimmte Protokolle, schriftlich fixierte Ergebnistypen, Berichte etc.

Der Auftragnehmer hat die von ihm im Zuge der Wahrnehmung seiner Aufgaben erbrachten Leistung in einer Form zu dokumentieren, die zu Vorlage bei prozessrelevanten Gremien und Entscheidern geeignet ist und auf deren vorgelegt zu werden und auf deren Grundlage Entscheidung gefällt werden können. Hierzu sind die durch den Auftraggeber bereitgestellten Vorgabe- und Nachweisdokumente als Templates zu nutzen.

Sollte Auftragnehmer Problems bearbeiten, die Auftraggeber betreffen, aber nicht in dessen ITSM-Tool abgebildet sind, stellt Aufragnehmer einen Report über diese Tickets zur Verfügung. Der Report enthält mindestens folgende Angaben umfassen:

- Zeitpunkt Eröffnung
- Nummer
- Titel
- Prio
- Status
- Bearbeitungsfortschritt

Der Report ist den jeweiligen Operations- oder Service Meetings zu besprechen. Die Besprechnungergebnisse sind im entsprechenden Protokoll zu dokumentieren.

7.3 Change-Management

Ist der Auftragnehmer bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?

Falls dies der Fall ist, sind für den vorliegenden Auftrag die Abschnitte 7.3 ff „Change-Management“ der ihnen vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

Das Change Management stellt sicher, dass standardisierte Methoden und Verfahren für eine termingerechte, effiziente und kostengünstige Planung / Koordination von Changes verwendet werden. Damit wird das Risiko für bestehende oder neue IT-Services minimiert und die fehlerfreie Umsetzung ermöglicht.

Die Prozesse und Verfahren des Change-Managements stellen sicher, dass Änderungen an IT-Services über einen fest definierten Ablauf umgesetzt werden. In diesen Prozessablauf sind alle betroffenen Lieferanten und Dienstleister (synonym Provider) integriert. Das Change-Management ist dabei das zentrale, steuerndes und dokumentierendes Kontrollorgan für Veränderungen, die direkten oder indirekten, wesentlichen Impact für die Erbringung der IT-Services haben können – unabhängig von Quelle bzw. Auslöser.

Der Change Management Prozess beinhaltet die Erfassung, Dokumentation, Genehmigung und Überwachung von Changes und stellt sicher, dass die Veränderungen geplant, effizient, kostengünstig und mit minimalen Risiken ausgeführt werden. Der Scope des Change Managements erstreckt sich hierbei über alle Klassen und Komponenten die der Auftraggeber in seiner „Configuration Management Data Base“ (CMDB) verwaltet

Für Veränderungen, die direkten oder indirekten, wesentlichen Impact für die Erbringung der IT-Services an die Kunden haben können, muss ein „RfC“ - Request for Change - gestellt werden.

7.3.1 Verantwortlichkeiten und Rollen im Change-Management

Ein Change kann durch Mitarbeiter des Auftraggebers oder autorisierte Mitarbeiter des Auftragnehmers (Providers) ausgelöst werden.

Aufgaben im Change Management sind in folgenden Rollen definiert und zugewiesen:

- Process Owner
- Change Manager (je Fachbereichsbetreuung (FBB) und Provider)
- Change Koordinator (je IT-Service)

Hierbei hat der Auftragnehmer zumindest die Rolle als Change-Koordinator für die von ihm verantworteten Leistungen wahrzunehmen, als auch in seiner eigenen Organisation entsprechende Verantwortlichkeiten für eine ebenegerechte Interaktion mit dem Auftraggeber implementiert haben. Darüber hinaus gehende Rollenwahrnehmung kann der Auftraggeber vertraglich verlangen.

Bei der im Rahmen seiner Leistungserbringung zu berücksichtigende Rollenwahrnehmung, hat der Auftragnehmer die Teilnahme an verschiedenen Gremien (Boards) zu berücksichtigen. U.a. ist für „übergreifende Changes“ (Definition hiernach) das Change Advisory Board der UIT (CAB UIT), dass sich aus den betroffenen Lieferanten (Providern), sowie Vertretern des Auftraggebers zusammensetzt.

7.3.2 Schnittstellen des Prozesses zu anderen ITSM-Prozessen

Das Change-Management hat eine Vielzahl organisatorischer Schnittstellen zu den anderen IT-Service Management-Prozessen des Auftraggebers. Der Auftragnehmer hat bei zur Erbringung seiner Leistung wahrzunehmenden Rolle, auch die Abstimmung (damit verbundene Aufwände und zeitliche Disposition) zu berücksichtigen. Diese berechtigen den Auftragnehmer nicht zur Geltendmachung zusätzlicher separater Aufwände.

Eine besonders enge Verzahnung besteht hierbei zwischen Change Management, Configuration Management und Release- und Deployment-Management.

Mittels der Schnittstelle zum Information Security Management wird sichergestellt, dass RfCs korrekt eingestuft werden.

Besondere Aufmerksamkeit ist daher der frühzeitigen Einbindung dieser Schnittstellenpartner zu schenken, um Changes aufwandsarm und effizient durchzuführen.

7.3.3 Merkmale und Klassifikationen für Changes

Changes werden anhand einer Reihe von Merkmalen klassifiziert. Diese Klassifizierungen können sich auf Merkmale des Changes als auch das betroffene Umfeld beziehen. Die Klassifizierung eines Changes bestimmt letztlich in welcher Art und Umfang der Change mit den Betroffenen und den Schnittstellenpartnern abzustimmen ist.

Wesentliche Merkmale und von Changes sind:

- Change-Kritikalität
  - Easy (Nur für CI-Change oder Non-Prod-Systeme)
  - Minor
  - Significant
  - Major
  - Emergency
- Change-Art
  - CI-Change
  - Info-Change
  - Infrastruktur, HW, SW, Daten und Wartung
- Change-Beteiligte
  - Single
  - Übergreifend
- Standard- und Sonderfälle
  - Major Change of Service
  - Standard Change
  - Emergency Change

7.3.4 Definition der Change-Arten

Vorgenannte Change-Arten sind wie folgt definiert:

CI-Change: Anwendbar für alle Änderungen in der CMDB, die kein Deployment (Änderung) in der Infrastruktur (Hard- und Software) erfordern. Änderungen, die ein Deployment erfordern, dürfen nicht über CI-Changes abgewickelt werden.

Infrastruktur-Change: Sind für die Durchführung von Änderungen an der Infrastruktur (Hard- und Software) zu verwenden. Jede Art von Änderungen in der CMDB kann im Rahmen eines Infrastruktur-Changes durchgeführt werden.

Info-Change: Dient zur Kommunikation und Zustimmung mit rein organisatorischem Charakter (z.B.: Vorankündigung eines Infrastruktur-Changes, Ankündigung/Anforderung eines Arbeitstages an z.B. einem gesetzlichen Feiertag, Ankündigung eines Wartungswochenendes). Der Info-Change kann kein Deployment (Änderung) in der Infrastruktur (Hard- und Software) bewirken.

7.3.5 Definition Change-Beteiligte

Single-Change: Bei Single Changes werden die Aktivitäten lediglich bilateral und unmittelbar zwischen dem beauftragenden Bereich des Auftraggebers und dem Auftragnehmer abgestimmt. Der Auftragnehmer kann nach erfolgter Abstimmung und Dokumentation die Umsetzung vornehmen, da die Folgen eines aus der Umsetzung des Changes auftretender Incident auf den unmittelbar an der Abstimmung beteiligten Bereich des Auftraggebers beschränkt bleibt.

Übergreifender Change: Ein übergreifender Change liegt vor, wenn durch die Umsetzung eines Changes mindestens ein zweiter Auftragnehmer in seiner Leistungserbringung oder ein anderer als der unmittelbar beauftragende Bereich des Auftraggebers bei der Nutzung von Leistungen betroffen ist. Die Freigabe von übergreifenden Changes erfolgt einzig und alleine durch das übergreifende CAB UIT. Der Auftragnehmer kann die Umsetzung erst nach dokumentierter Freigabe durch das Gremium die Umsetzung des Changes vornehmen. Entsprechende Aufwände und zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen.

7.3.6 Standard- und Sonderfälle

Major Change of Service: Changes die einen wesentlichen („major“) Impact auf einen IT-Service haben, müssen zwingend durch die einen Prozess des Service-Life-Cycle Managements. Wesentlich ist ein Change in folgenden Fällen:

- ein IT-Service wird neu im Service Katalog aufgenommen,
- hoher Impact auf Services (z.B. neue Technologie)
- ein IT-Service wird bzw. seine Service Komponenten (Managed Services) werden wesentlich geändert (in Art und Umfang, z.B. Providerwechsel),
- oder ein IT-Service wird nicht mehr über den Service Katalog angeboten.

Die wesentliche Änderung eines IT-Service bzw. seiner Service Komponenten (Managed Services) in Art und Umfang, umfasst dabei Änderungen an folgende Attributen in der Configuration Management Data Base

- der Configuration Item-Klasse (CI-Klasse):
- IT-Service
- oder Managed Service

Standard Change: Standard Changes tragen dazu bei, Prozessausführungen zu beschleunigen und dadurch die Effizienz des Change Management zu fördern. Für einen Standard Change wurde die erforderliche Autorisierung vorab gegeben. Er kann bei Änderungen derselben Art bei Bedarf abgerufen werden und muss nicht nochmals autorisiert werden.

Ein Test vor der Implementierung ist nicht erforderlich für Standard Changes. Dieser Test wurde während der Definition des Standard Changes durchgeführt. Per Definition muss ein Standard Change ein geringes Risiko haben. Ein nachträglicher Post Implementation Review muss auch für Standard Changes durchgeführt werden. Das heißt, nachdem ein Change implementiert wurde, muss der definierte Test durchgeführt und dokumentiert werden, um zu ermitteln, ob der Change erfolgreich war.

Kriterien für eine Klassifizierung als Standard-Change sind:

- Bekanntes, leicht kalkulierbares und geringes Risiko (keine weitreichenden Auswirkungen auf geschäftskritische Assets (Daten, Prozesse, Systeme…) oder Security Aspekte)
- Bekannte Kosten
- Mehrfach erfolgreich durchlaufene und gut implementierte Procedures (Change Implementation Plan (CIP), Backout Planung). Alle Aktivitäten, Abhängigkeiten, Verantwortlichkeiten und Impact sind bekannt
- Mehrfach erfolgreich durchlaufene und gut implementierte „Post Implementation Test Procedure“
- Klar definierte Rollen und Zuständigkeiten
- Kein fachbereichsübergreifender Impact

- Vorabgenehmigt durch Dataowner und verantwortlichen Change Manager (die Verantwortung für den Change bleibt davon unberührt)

Die notwendigen Eingaben für einen RfC können im Rahmen eines Standard Changes vereinfacht werden. Standard Changes werden bereits im Vorfeld modelliert und können dann bei Bedarf abgerufen werden. Die initiale Genehmigung eines Standard Changes erfolgt durch den Change Manager und den Dataowner.

Emergency Change: Ein Emergency Change zeichnet sich durch besondere Kritikalität (Gefährdung der Produktion) aus. Da es sich meist um zeitkritische Changes handelt, erfolgt die Kommunikation über zentrale E-Mail Verteiler. Je nach betroffenen Services werden spezifische E-Mail Verteiler genutzt.

Übergreifend ist der Verteiler UIT_Emergency_Changes@union-investment.de zu nutzen. Prinzipiell hat jeder Beteiligte ein „Veto- Recht“.

Nach Abstimmung bzw. Durchführung erfolgt eine Dokumentation des Changes im Change-Management Tool des Auftraggebers.

Entsprechende Aufwände und zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen.

7.3.7 Request for Change (RfC) erstellen, genehmigen und einreichen

Das Vorhaben einer Änderung an einem oder mehreren Komponenten innerhalb eines IT Service durchzuführen wird als RfC beim Change Koordinator eingereicht und ist daher die erste Aktivität um den Change-Prozess zu starten. Ein RfC ist noch kein Change, sondern die Ankündigung und Beschreibung (u.a. Art, Ziel, Auslöser, Zeitplan) einer möglichen Veränderung sowie deren Klassifizierung.

Erst nach dem Prozessschritt „Change erstellen“ wird der RfC durch den Change Koordinator / Manager als Antragsdokument angenommen und in seinen weiteren Lebenszyklus als Change weitergeführt.

7.3.8 Change planen und bewerten

In diesem Subprozess wird der RfC durch den Change Koordinator überprüft, mit dem betroffenen Managed Service verknüpft, hinsichtlich seines Impacts bewertet und einer detaillierten Planung bzw. Kontrolle der Change Implementation Plan (CIP) und Backout Planung unterzogen.

Je nach Change-Kritikalität (Minor, Significant, Major, Emergency), -Priorität und -Art wird der Change – insbesondere bei Bearbeitung sicherheitsrelevanter Changes - durch unterschiedliche Prozesse mit unterschiedlichen Prozessangaben weiter bearbeitet

In folgenden Bereichen der Change-Bewertung ist für Changes der Klassifikation Major und Significant eine ausreichende Dokumentationsgüte zur Unterstützung der Umsetzungsqualität zwingend notwendig und vom Auftragnehmer (insbesondere für übergreifende Changes) für die Vorlage im Rahmen des Post Implementation Review (PIR) bzw. dem CAB UIT vorzulegen:

- Change Implementation Plan (CIP)
- Impact Analyse / CMDB-Information
- Backout sowie Rollbackplan, falls abweichend vom Backout-Plan.
- Planung
- Backout Test
- Post Implementation Review (PIR) durch den Change Koordinator.

7.3.9 Change abstimmen

Alle Änderungen der Change-Arten: Infrastruktur, Hardware, Software, Daten und Wartung, die die Produktion betreffen – auch wenn diese vom Auftragnehmer initiiert sind, sind vor Produktivnahme zu testen und durch den verantwortlichen Dataowner des Auftraggebers zu genehmigen.

Der Auftragnehmer muss hierzu die von ihm bereitgestellten Komponenten in eigener Verantwortung testen und die Abnahmebereitschaft für die Einholung der Genehmigung gegenüber dem Dataowner beim Auftraggeber in Textform anzeigen.

Vor Produktivnahme ist im RfC-Record zu dokumentieren, ob die im Rahmen des Changes betroffenen Komponenten erfolgreich die erforderlichen Tests durchlaufen haben. Ferner ist in diesem RfC-Record anzugeben in welcher Form und welchem Ort die Testdokumentation abgelegt ist. In Abhängigkeit vom Änderungsinhalt (Change-Inhalt) sind verschiedene vom Auftraggeber definierte Teststufen zu berücksichtigen.

Danach wird der Change zur Abstimmung (Prüfung auf mögliche Auswirkungen auf andere IT Services) den Change Managern des Auftraggebers und den evtl. betroffenen Auftragnehmern (Providern) zur Genehmigung vorgelegt. Diese Vorlage erfolgt per Mailbenachrichtigung und einem Verweis in das Change Management System des Auftraggebers.

Das Abstimmungsergebnis unterliegt dabei insbesondere dem definierten Umsetzungszeitraum. Änderungen des Umsetzungszeitraumes nach Initiierung der Abstimmung führen zu einer erneuten Abstimmung unter Berücksichtigung des geänderten Zeitraumes. Entsprechende Aufwände sowie die zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen.

7.3.10 Umsetzung genehmigen

Nach erfolgreicher Abstimmung kann die Genehmigung zur Umsetzung des Change erfolgen.

In Abhängigkeit von Change-Ausmaß (Single oder übergreifend) und -Klassifizierung, ist der Change durch eine weitere Instanz (z.B. UIT-Change Advisory Board) abschließend zur Umsetzung freizugeben. Dabei ist das Vier-Augen-Prinzip im Rahmen der Change-Bewertung und Change-Freigabe zwingend für alle Infrastruktur-Changes einzuhalten, bzw. Ausnahmen revisionssicher im Change zu dokumentieren.

Den Auftragnehmern (Provider) obliegt es den Change-Prozess durch Benennung eines Provider Change Managers, sowie Vertretern zu unterstützen.

Der Provider Change Manager ist Ansprechpartner für die richtige Klassifizierung bzw. Change-Abstimmung und Change-Genehmigung der eingereichten Changes.

Zur Nachweisbarkeit erfolgt diese Abstimmung mit entsprechender Protokollierung im Change-Management-Tool des Auftraggebers. Entsprechende Aufwände sowie die zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen.

7.3.11 Change durchführen

Sobald für einen Change alle für die Umsetzung erforderlichen Genehmigungen vorliegen, wird dieser im Zustand „in Umsetzung“ ausgewiesen. In diesem Zustand können die beabsichtigten Änderungen durchgeführt werden. Im Zustand “in Umsetzung“, ist es nicht mehr möglich, Änderungen an der Dokumentation zur Change-Planung (CIP, Backout Planung, Umsetzungszeitraum, Impact Analyse) vorzunehmen. Entsprechende Aufwände sowie die zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen. Nach erfolgreicher Umsetzung erfolgt die Rückmeldung an das Change Management.

7.3.12 Post Implementation Review (PIR) und Change abschließen

Der Post Implementation Review wird vom Change Koordinator durchgeführt und dient der Nachbetrachtung des implementierten Changes. Ziel der PIR ist es sicherzustellen, dass alle Aktivitäten vollständig und erfolgreich abgeschlossen wurden und keine aktuellen Risiken in der Produktionsumgebung bestehen. Werden Mängel im PIR festgestellt, so werden diese und ggf. getroffene Maßnahmen im Rahmen des PIR nachvollziehbar dokumentiert.

Nach erfolgreicher Umsetzung und Beurteilung des Changes wird der Change durch den Change Manager abgeschlossen.

Der Auftragnehmer hat die von ihm im Zuge der Umsetzung des Changes erbrachten Leistung in einer Form zu dokumentieren, die geeignet ist, dem PIR vorzulegen und die Entscheidung über die

Abgeschlossenheit des Changes zu fällen. Hierzu sind die durch Auftraggeber bereitgestellten Vorgabe- und Nachweisdokumente als Templates zu nutzen.

Werden im PIR Mängel bei der vom Auftragnehmer durchgeführten Umsetzung des Changes festgestellt, so unternimmt der Auftragnehmer die Beseitigung dieser Mängel entsprechend der Fehlerklassen gem. Vertragsbedingungen, bis eine Abnahme im PIR erfolgt ist. Entsprechende Aufwände sowie die zeitliche Disposition hat der Auftragnehmer für seine Leistungserbringung einzuplanen.

8 IT-Sicherheitsstandards: Anforderungen an Supplier

Erbringt der Auftragnehmer Leistungen in einem der folgenden Themenfelder, bzw. nimmt dort Rollen und Aufgaben wahr: Infrastruktur-Betrieb, Anwendungsentwicklung/-Implementierung, technische Anwendungsbetreuung, fachliche Anwendungsbetreuung oder sonstige Anwendungsbetreuung?

Falls dies der Fall ist, sind für den entsprechenden Auftrag die Abschnitte 8ff „IT-Sicherheitsstandards: Anforderungen an Supplier“ der vorliegenden „Liefer- und Leistungsbedingungen“ einschlägig und als Teil des Auftrages zu beachten.

Erbringt der Auftragnehmer Leistungen in einem der folgenden Themenfelder: Infrastruktur-Betrieb, Anwendungsentwicklung/-Implementierung, technische Anwendungsbetreuung, fachliche Anwendungsbetreuung oder Bereitstellung einer SaaS-Lösung, bzw. nimmt dort Rollen und Aufgaben wahr, hat er die damit verbundenen spezifischen Anforderungen zur IT-Sicherheitsstands des Auftraggebers zu erfüllen. Die Anforderungen zur IT-Sicherheitsstands des Auftraggebers orientieren sich dabei im Wesentlichen an den Anforderungen der ISO-Normen 27001 bzw. 27002.

Die Anforderungen sind hierbei in einer Form beschrieben die es dem Auftragnehmer ermöglicht, auf bereits bei ihm etablierte und bewährte Verfahren bzgl. der Informationssicherheit zurückzugreifen und im Rahmen der technischen Umsetzung aktuelle Technologien einzusetzen.

In Folge dessen bleibt der Auftragnehmer dafür verantwortlich eigene interne Sicherheitsmaßnahmen zu planen, steuern und zu überwachen. Er muss ein geeignetes Sicherheitsmanagement, z.B. nach ISO 27001 oder BSI Grundschutz, vorhalten und dessen Wirksamkeit gegenüber der beauftragenden Gesellschaft der Union Investment Gruppe nachweisen.

8.1 Steuerungsprozess bei Vertragsanbahnung und während der Betriebsübergabe

Bereits während des Auswahlprozesses bzw. Vertragsanbahnungsphase erhält der potentielle Auftragnehmer von dem Auftraggeber eine Beschreibung des geforderten Sicherheitsniveaus in Form eines Anforderungskatalogs (Checkliste).

Damit ein potentieller Auftragnehmer im weiteren Verlauf des Auswahlverfahrens Berücksichtigung finden kann, muss er die Anforderungen seinerseits auf Erfüllbarkeit prüfen. Er muss gegenüber dem Auftraggeber mitteilen in welcher Art und Umfang er die Anforderungen umsetzen kann. Hierzu sind durch den Auftragnehmer zumindest folgende Unterlagen vorzulegen, damit der Auftraggeber, bzw. das Information Security Office der Union Investment Gruppe eine Bewertung vornehmen kann, ob durch die beschriebenen Maßnahmen die Erfüllung der Sicherheitsanforderungen gewährleistet wäre:

- Übersicht der seitens des Auftragnehmers vorhandenen bzw. zu erstellenden Unterlagen gemäß den Berichtsanforderungen des vor genannten Anforderungskataloges (Checkliste).
- Konzepte zur Implementierung, die eine grundsätzliche Beurteilung der Effektivität und Angemessenheit der geplanten Maßnahmen bezogen auf die Sicherheitsanforderungen zulassen.
- Auflistung und Begründung der nicht umsetzbaren/nicht erfüllbaren Anforderungen.

Spätestens vor Betriebsübergabe müssen zusätzlich zu den o.g. Dokumenten die zugehörigen Nachweise, die ebenfalls durch den Auftraggeber bzw. das Information Security Office des Auftraggebers geprüft und bewertet werden. Im Rahmen der durchzuführenden Prüfungen können weitere Unterlagen für den Abschluss der Prüfung angefordert werden. Insofern die Prüfung ergibt, dass die Anforderungen nur durch Maßnahmen des Auftragnehmers erreicht werden, die er zum Zeitpunkt der Prüfung erst noch umsetzen muss, so können diese ihm als umzusetzende Maßnahmen auferlegt werden. Der Auftragnehmer ist nicht berechtigt aus der Erfüllung der Anforderungen und der Umsetzung auferlegter Maßnahmen entstehende Aufwände und Kosten zusätzlich zu seiner angebotenen Vergütung in Rechnung zu stellen.

Spätestens mit Erlangung des Zugriffs auf die schutzbedürftigen Informationen (bzw. Systeme etc.) muss der Auftragnehmer die ihm auferlegten Maßnahmen umsetzt haben.

8.2 Berichtswesen (Reporting)

Der Auftragnehmer hat die ordnungs- und vertragsgemäße Leistungserbringung durch turnusgemäße Vorlage der mit dem Auftraggeber definierten Berichte, Kennzahlen, Betriebsdokumentationen sowie andere vom Auftraggeber als geeignet erachtete Nachweise nachzuweisen. Die Spezifikationen der erforderlichen Inhalte sind im Nachfolgenden angegeben.

Die turnusgemäß zu erstellenden Berichte listen die spezifizierten Ereignisse je Berichtszeitraum auf. Sofern nichts anderes vereinbart ist, umfasst der Berichtszeitraum immer ein Quartal. Die turnusmäßig zu erstellenden Berichte haben in ihrer Struktur unverändert zu bleiben, damit ein Vergleich mit den Vorperioden möglich ist. Vorgelegte Berichte sind über die Laufzeit des Leistungsbezuges zu historisieren. Die Bereitstellungszeit sowie die Art der Bereitstellung (in einem Portal, per E-Mail etc.) richten sich nach den vertraglichen Vereinbarungen. Dabei muss die Art der Bereitstellung der Berichte dem Auftraggeber der Union Investment Gruppe ermöglichen, die Berichte als Datei herunterzuladen und die Berichtsdaten für eine mechanisierte Weiterverarbeitung zu extrahieren.

Die sonstigen Nachweise sind grundsätzlich so bereitzustellen, dass sie jederzeit durch den Auftraggeber eingesehen werden können.

Zusätzlich zu den turnusmäßigen Berichten können von dem Auftraggeber Berichte im Zusammenhang mit sicherheitsrelevanten Ereignissen vom Auftragnehmer angefordert werden.

8.3 Audits

Das Sicherheitsmanagement des Auftraggebers muss jederzeit in der Lage sein, die zur Erfüllung der hier genannten Anforderungen ergriffenen Maßnahmen verifizieren und bewerten zu können. Als wichtigste Methode führt der Auftraggeber sogen. Security Audits beim Auftragnehmer durch. Im Rahmen eines solchen Audits werden die vom beim Auftragnehmer vorgelegten Nachweise verifiziert und die Erfüllung der Vorgaben geprüft.

Die vom Auftragnehmer einzuräumenden Audit- Prüfrechte können dabei je Anwendungsfall aufgrund unterschiedlicher gesetzlich Vorgaben variieren. Bei Auslagerungen, ist daher die Berechtigung zur Durchführung von Audits durch den Auftraggeber oder von ihm beauftragter Dritter aus dem Kreis der zur Verschwiegenheit verpflichteten Berufsgruppen (Wirtschaftsprüfungsgesellschaften) beim Auftragnehmer erforderlich. Der Auftragnehmer räumt die erforderlichen Prüfungsrechte spätestens mit Aufnahme der Leistungserbringung ein.

8.4 Teilnahme an Service Meetings

Für regelmäßige Abstimmungen nehmen Vertreter des Auftraggebers und des Auftragnehmers an den regelmäßig stattfindenden Service Meetings gemäß Outsourcing-Governancemodell (vgl. Outsourcing-Rahmenvertrag) teil.

8.5 IT Sicherheitsanforderungen

8.5.1 Umgang mit Passwörtern

	Standard Passwort-Policy	Alternative[2] Passwort-Policy	Mobile Endgeräte
Länge	Mindestlänge 12 Zeichen	Mindestlänge 8 Zeichen	
Bedingungen	Es dürfen keine Bestandteile des Anmeldenamens enthalten sein		• Es dürfen keine einfachen Passwörter verwendet werden • Löschung des Geräts nach 10 Fehlversuchen • Face ID
Zeichengruppen	4 von 4 der folgenden Zeichengruppen müssen enthalten sein	3 von 4 der folgenden Zeichengruppen müssen enthalten sein	
	• **Großbuchstaben** (A bis Z, ohne Umlaute) • **Kleinbuchstaben** (a bis z, ohne Umlaute) • **Ziffern** (0 bis 9) • **Nicht-alphanumerische Zeichen** (z.B. !, $, #, %)		Alphanumerische Zeichen (Klein-/Großbuchstaben, Ziffern)
Wechsel Zeitraum	Bei Bedarf, Verlust	Jede 90 Tagen	Bei Bedarf, Verlust
Unterschied zum früheren Passwort	Letzte 5 benutzte Passworte	Letzte 15 benutzte Passworte	-

[2] Alternative Passwort-Policy wird verwendet, wenn die Standard-Policy in der Anwendung/Zielsystem technisch nicht umgesetzt werden kann.

Für die Benutzeraccounts dürfen keine Passwörter aus dem privaten Umfeld des IT-Benutzers verwendet werden, wenn der private Account und der Union-Account so ähnlich oder gar gleich sind, dass sie durch Außenstehende derselben Person zugeordnet werden können.

 Bei Kenntnis oder Verdacht auf Passwort-Kompromittierung (d.h. ein Dritter könnte in Besitz des Passworts gelangt sein) ist die Führungskraft und der Information Security Officer zu informieren.

Die UIG behält sich das Recht vor, eine gewisse Passwortkomplexität abhängig von der jeweiligen Anwendung technisch zu erzwingen.

8.5.2 Anforderungskatalog (Controls) des IT-Security Managements

8.5.2.1 Vereinfachtes Vorgehen zu den Anforderungen der Richtlinie RL-5069

Grundsätzlich gelten für Auftragnehmer die in der nachfolgenden Liste genannten Anforderungen zu IT-Sicherheitsaspekten. Die dort genannten Anforderungen sind abhängig vom Leistungsbild und dem Kontext des Einsatzbereiches des Auftragnehmers (Konfektionierung) durch ihn verbindlich einzuhalten. Die einzuhaltenden Kontrollen leiten sich aus ihrer Anwendbarkeit ab und ergeben sich dann aus der Konfektionierung und der Zuordnung (per Kreuz) aus der nachfolgenden Liste der Kontrollen. Die vertragliche Vereinbarung der Konfektionierung kann übergeordnet im Rahmenvertrag, in der Rahmenkonditionenvereinbarung oder mit der jeweiligen Einzelbeauftragung (z.B. Leistungsschein) erfolgen. Solange und soweit vertraglich keine Konfektionierung vereinbart ist, sind alle Kontrollen, unabhängig vom Leistungsbild und dem Kontext des Einsatzbereiches des Auftragnehmers, gemäß der nachfolgenden Liste durch Auftragnehmer einzuhalten.

Alternativ zum vereinfachten Vorgehen gemäß dieser Ziffer 8.5.2.1 kann auf Anforderung von Auftraggeber das erweiterte Vorgehen gemäß Ziffer 8.5.2.2 angewendet werden.

Anforderung der Richtlinie RL-5069 (ISO27001/2)						
ID	**Kontrolle**	Konfektionierung				
		Infrastruktur-Betrieb	Anwendungs-Entwicklung/ -Implementierung	technische Anwendungs-betreuung	fachliche Anwendungs-betreuung	SaaS
5 Sicherheitsleitlinie (ID.5 Information security policies)						
ID.05.01.01-01	Eine Richtlinie/Leitlinie "Informationssicherheit" ist als Teil der schriftlich fixierten Ordnung definiert, die die wesentlichen Ziele der Informationssicherheit (Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen) enthält.	x	x	x	x	x
ID.05.01.01-02	Eine Richtlinie/Leitlinie "Informationssicherheit" ist durch den Vorstand des Suppliers freigegeben.	x		x	x	x
ID.05.01.01-03	Die Richtlinie/Leitlinie "Informationssicherheit" wird durch weitere Richtlinien und Arbeitsanweisungen zur Informationssicherheit ergänzt. Die Richtlinie/Leitlinie "Informationssicherheit" enthält einen Verweis auf weiterführende Dokumente.	x		x	x	x
ID.05.01.01-04	Die geltenden Richtlinien/Arbeitsanweisungen sind verständlich und zielgruppenorientiert formuliert. Die Dokumente sind wirksam kommuniziert und bei Bedarf leicht auffindbar.	x		x	x	x
ID.05.01.01-05	Im Rahmen der IT-Strategie des Unternehmens wird explizit auf die Rolle und die Bedeutung der Informationssicherheit innerhalb der Organisation eingegangen.	x				x
ID.05.01.01-06	Die Richtlinie und Verfahren zur Informationssicherheit stehen im Einklang mit der Geschäftsstrategie und dem Risikoappetit des Dienstleisters.	x		x		x
ID.05.01.02-01	Die erstellten Richtlinien und Arbeitsanweisungen sind mindestens einmal pro Jahr auf ihre inhaltliche Angemessenheit zu überprüfen und bei Bedarf zu aktualisieren.	x	x	x	x	x
ID.05.01.02-02	Allen erstellten Richtlinien und Arbeitsanweisungen ist eine verantwortliche Rolle zuzuweisen, die die Erstellung, Überprüfung und laufende Aktualisierung sicherstellt.	x		x	x	x
6 Organisation der Informationssicherheit (ID.6 Organization of information security)						
ID.06.01.01-01	Rollen und Verantwortlichkeiten im Kontext des Informationssicherheitsmanagements sind zu definieren und als Teil der schriftlich fixierten Ordnung zu dokumentieren.	x		x	x	x
ID.06.01.01-02 (Änderung)	Es ist ein IT-Sicherheitsbeauftragter (ISO) benannt, der fachlich und disziplinarisch unabhängig von der operativen IT (Entwicklung und	x		x	x	x

	Betrieb) ist. Der IT-Sicherheitsbeauftragte (ISO) agiert damit als 2. Verteidigungslinie (2nd Line of Defense).					
ID.06.01.01-03	Der IT-Sicherheitsbeauftragte (ISO) berichtet regelmäßig, mindestens vierteljährlich, an (mindestens) zwei unabhängige Vorstandsressorts.	x		x	x	x
ID.06.01.01-04	Es ist eine dezentrale Rolle zur Informationssicherheit etabliert, die die Interessen der Fachabteilung bei Schutz der Informationsverarbeitung vertritt.	x		x	x	x
ID.06.01.01-05	Es ist eine dezentrale Rolle zur Informationssicherheit etabliert, die die Umsetzung der Anforderungen bzgl. Informationssicherheit für die IT-Assets verantwortet. Die dezentrale Rolle agiert als 1. Verteidigungslinie (1st Line of Defense).	x		x	x	x
ID.06.01.02-01	Bei der Definition von Rollen und Verantwortlichkeiten sind Funktionstrennungsaspekte zu berücksichtigen. Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind zu trennen, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch von IT-Assets zu reduzieren.	x	x	x	x	x
ID.06.01.03-01	Der Supplier hat Kontakte zu den relevanten Aufsichts- und Strafverfolgungsbehörden etabliert. Datenschutz Hinweis*: Der Supplier hat einen adäquaten Betroffenenrechteprozess implementiert (Informationspflichten, Auskunft, Löschung, etc.) (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x		x	x	x
ID.06.01.04-01	Geeignete Kontakte zu speziellen Interessengruppen oder anderen Experten-Sicherheitsforen und professionellen Verbänden müssen gepflegt werden.	x		x	x	x
ID.06.01.05-01	Die Relevanz für das Thema Informationssicherheit ist gemäß einer definierten Projektmanagementmethodik in einer frühen Phase des Projektes zu bewerten. Auf Basis der initialen Bewertung werden Projekte durch den IT-Sicherheitsbeauftragten (CISO) begleitet.	x				x
ID.06.01.05-02	Der IT-Sicherheitsbeauftragte (CISO) erhält einen periodischen Überblick über aktuell laufende und geplante Projekte (Projektvorhaben).	x		x	x	x
ID.06.02.01-01	Eine Leitlinie zu mobilen Geräten ist zu erstellen. Die Umsetzung der dort definier-ten Vorgaben ist durch den IT-Sicherheitsbeauftragten (CISO) formal auf Basis dieser Mindeststandards zu überwachen. Dabei sind die besonderen Risiken durch die mobile Nutzung angemessen zu berücksichtigen.	x		x	x	x
ID.06.02.02-01	Tele- und Heimarbeit ist unzulässig, es sein denn der Supplier hat eine schriftliche Vereinbarung mit der UIG getroffen.	x		x	x	x
7 Personal-Sicherheit (ID.7 Human resource security)						
ID.07.01.01-01	Die Angaben von Personen im Bewerbungsprozess sind vor der Anstellung hinsichtlich der, für die zu besetzenden Stelle, notwendigen Qualifikationen/Kompetenzen zu überprüfen.	x		x	x	x
ID.07.01.01-02	Die Identität einer Person ist vor Eintritt ins Unternehmen vom Supplier zu verifizieren.	x		x	x	x
ID.07.01.02-01	Arbeitsverträge enthalten Klauseln zur Vertraulichkeit/Geheimhaltung geschäftlicher Informationen, den Umgang mit Informationen sowie Verweise auf relevante gesetzliche / regulatorische Pflichten. Datenschutz Hinweis*: Der Supplier hat seine Mitarbeiter schriftlich auf den vertraulichen und datenschutzkonformen Umgang mit personenbezogenen Daten verpflichtet. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x	x	x	x	x
ID.07.01.02-02	Vereinbarungen mit Dienstleistern bzw. den vom Dienstleister eingesetzten Personal enthalten Klauseln zur Vertraulichkeit/Geheimhaltung geschäftlicher Informationen, den Umgang mit Informationen sowie Verweise auf relevante gesetzliche / regulatorische Pflichten.	x	x	x	x	x
ID.07.02.02-01	Es existiert eine adressatengerechte Kommunikation inkl. Schulungsangeboten (Präsenz/Online) zur Informationssicherheit für alle Mitarbeiter. Darin werden die wesentlichen Pflichten der Mitarbeiter auf Basis der Vorgaben zur Informationssicherheit vermittelt.	x		x	x	x
ID.07.02.02-02	Es ist sicherzustellen, dass die definierten dezentralen Rollen der Informationssicherheit die spezifisch für ihre Aufgabe erforderlichen Kenntnisse haben.	x		x	x	x

ID.07.02.02-03	Die für die (Weiter-) Entwicklung und den Betrieb eines IT-Assets oder Supporting Assets notwendigen Qualifikationen sind definiert.	x		x	x	x
ID.07.02.03-01	Es existiert innerhalb des Suppliers ein disziplinarischer Prozess für die Ahndung von Informationssicherheitsverstößen.	x		x	x	x
ID.07.03.01-01	Es existieren definierte Regelungen hinsichtlich Anwendbarkeit der definierten Anforderungen nach Ende der Vertragsbeziehung.	x		x	x	x
8 Asset Management (ID.8 Asset management)						
ID.08.01.01-01	Der Supplier pflegt ein Inventar, in dem alle Information Assets, IT-Assets sowie Supporting Assets des Suppliers erfasst sind.	x				x
ID.08.01.01-02	Für jedes IT-Asset ist mindestens festzulegen, ob rechnungslegungs-, steuerungsrelevante oder personenbezogene Information Assets verarbeitet werden. Die bei der Verarbeitung eingesetzten IT-Assets sind entsprechend zu klassifizieren (Vererbung).	x				x
ID.08.01.02-01	Für jedes Asset des Suppliers ist ein Asset-Eigentümer benannt.	x		x		x
ID.08.01.03-01	Es existieren Richtlinien für die Benutzer von IT-Assets (z. B. Benutzerrichtlinie), die Regeln für den Gebrauch der IT-Assets definieren.	x		x		x
ID.08.01.04-01	Der Supplier hat einen Prozess definiert, der die Rückgabe aller IT-Assets bei Beendigung des Beschäftigungsverhältnisses sicherstellt. Der Prozess umfasst auch die Beendigung von Dienstleistungsverhältnissen.	x		x	x	x
ID.08.01.04-02	Die Rückgabe von IT-Assets bei Beendigung des Beschäftigungsverhältnisses wird nachvollziehbar dokumentiert.	x		x	x	x
ID.08.02.01-01	Information Assets sind gemäß ihrer Vertraulichkeit sowie relevanten regulatorischen Anforderungen nach Verfahren zu klassifizieren, welche durch die UIG definiert werden. Datenschutz Hinweis*: Die Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art 5 DS-GVO werden bei jeder Verarbeitung personenbezogener Daten berücksichtigt. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x		x	x	x
ID.08.02.02-01	Sofern eine Kennzeichnung von Dokumenten erforderlich ist, ist diese so anzubringen, dass deren Vertraulichkeit leicht erkennbar ist. Die Angabe der Vertraulichkeit erfolgt entweder durch das Kürzel zusammen mit der Bezeichnung der Vertraulichkeitsklasse oder nur durch das Kürzel (Beispiel: gültig sind die Kennzeichnungen „C2“ oder „C2 - Vertraulich“, aber nicht „Vertraulich“ ohne die An-gabe „C2“).	x		x	x	x
ID.08.02.03-01	Der Supplier hat auf Basis der Anforderung zur Informationsklassifizierung Vorgaben zum Umgang mit Information Assets definiert.	x		x	x	x
ID.08.02.03-02	Der Supplier hat auf Basis der Anforderung zur Informationsklassifizierung risikoorientiert Maßnahmen zum Schutz von Information Assets vor unberechtigter Weitergabe (Data Loss Prevention) umgesetzt.	x		x	x	x
ID.08.03.01-01	Es müssen verbindliche Handlungsanweisungen für den Umgang mit Medien existieren.	x		x	x	x
ID.08.03.02-01	Datenträger sind nach Ende der Nutzungsdauer im Rahmen eines definierten Prozesses zu löschen. Werden Datenträger keiner weiteren Nutzung zugeführt so ist alternativ eine sichere Entsorgung vorzunehmen.	x		x	x	x
ID.08.03.03-01	Datenträger sind während des Transports risikoorientiert vor unbefugtem Zugriff oder Missbrauch jeglicher Art zu schützen.	x		x	x	x
9 Zugangs- und Zugriffskontrolle (ID.9 Access control)						
ID.09.01.01-01	Die Anforderungen an die Zugangs- und Zugriffskontrollen sind durch eine schriftlich fixierte Vorgabe zu regeln.	x		x	x	x
ID.09.01.01-02	Jede Anwendung (ODV und IDV) verfügt über ein dokumentiertes Berechtigungskonzept verfügen, das alle Rollen, Benutzergruppen, Benutzer und deren Zugriffsrechte enthält.			x	x	x
ID.09.01.02-01	Der Zugriff auf technische Netzwerkdienste wird für Benutzer durch technische Maßnahmen kontrolliert. Die Maßnahmen sind in einer schriftlichen Vorgabe definiert.	x				x
ID.09.02.01-01	Die Identität einer realen/natürlichen Person ist vor der Einrichtung eines zugehörigen Benutzers zu bestätigen	x		x		x
ID.09.02.01-02	Bei Zugriff auf ein IT-Asset ist der Benutzer eindeutig zu identifizieren. Dies geschieht beispielsweise über seine Benutzerkennung.			x		x

ID.09.02.01-03	Bei Nutzung von Single-Faktor-Authentifizierung ist ein hinreichend komplexes/ langes Passwort oder biometrisches Verfahren zu verwenden, sofern Maßnahmen zur Erkennung kompromittierter Anmeldedaten etabliert sind. Alternativ ist das Passwort spätestens alle 90 Tage zu wechseln.	x		x		x
ID.09.02.01-04	Jede Benutzerkennung ist genau einer realen/natürlichen Person zugeordnet. Dies gilt auch für Administratorkennungen.	x		x		x
ID.09.02.02-01	Anträge zur Erlangung oder Änderung von Berechtigungen auf Anwendungen (ODV und IDV) sind mindestens nach dem 4-Augen-Prinzip zu bearbeiten. Die Bedarfsfreigabe (formale Genehmigung durch disziplinarischen Vorgesetzen) oder Zulässigkeitsfreigabe (durch Informationseigentümer) hat getrennt von der technischen Umsetzung des Antrags durch (Berechtigungs-) Administratoren oder Berechtigungssysteme zu erfolgen.	x		x		x
ID.09.02.02-02	Zugriffsrechte sind auf Basis von Rollen oder Benutzergruppen zu vergeben. Die Zuweisung von einzelnen Zugriffsrechten (Berechtigungsobjekte) an Benutzer ist zu vermeiden.	x		x		x
ID.09.02.02-03	Anträge zur Erlangung oder Änderungen von Berechtigungen auf Anwendungen (ODV und IDV) sind nachvollziehbar zu dokumentieren.	x		x		x
ID.09.02.02-04	Alle für ein IT-Asset verfügbaren Zugriffsberechtigte (Benutzer und technische Nutzer) und die damit verbundenen Rechte und Funktionalitäten sind aufzulisten. Die Erfordernis der eingerichteten Zugriffsberechtigte und die damit verbundenen Rechte und Funktionalitäten sind mindestens einmal jährlich zu überprüfen (Rezertifizierung). Kritische IT-Berechtigungen sind mindestens halbjährlich zu überprüfen. Kritische IT-Berechtigungen sind durch die Supplier risikoorientiert zu definieren und zu dokumentieren.	x		x		x
ID.09.02.03-01	Administrative Tätigkeiten sind über ein personalisiertes Benutzerkonto durchzuführen.	x		x		x
ID.09.02.03-02	Für administrative Tätigkeiten sind gesonderte Benutzerkonten einzurichten. Diese Kennungen sind logisch von normalen Benutzerkonten zu trennen.	x		x		x
ID.09.02.03-03	Die Verwendung administrativer Benutzerkonten wird manipulationssicher protokolliert und regelmäßig durch unabhängige Dritte überprüft.	x		x		x
ID.09.02.04-01	Daten zur interaktiven Anmeldung, sowie zur Authentifizierung solcher Anmeldungen am Zielsystem werden nicht im Klartext gespeichert.	x		x		x
ID.09.02.04-02	Müssen Daten zur automatischen (bspw. skriptgesteuerten) Anmeldung an einem IT-Asset gespeichert werden, so sind diese nach dem Stand der Technik zu schützen.	x		x		x
ID.09.02.04-03	Das Passwort, das bei der Neuanlage eines Benutzerkontos vergeben wird, wird nach dem Stand der Technik geschützt. Insbesondere sind leicht zu erratende Passwörter zu unterbinden. Das Passwort ist dem zugehörigen Benutzer auf sicherem Weg mitzuteilen.	x		x		x
ID.09.02.04-04	Bei Neuanlage eines Benutzerkontos oder Passwortrücksetzung generierte Initialpasswörter sind nach der ersten Anmeldung zu ändern.	x		x		x
ID.09.02.05-01	Alle auf dem IT-Asset eingerichteten Zugriffsrechte eines Benutzers sind regelmäßig zu überprüfen. Der Zeitraum orientiert sich an der Kritikalität der Zugriffsrechte. Insbesondere sind in diesem Zusammenhang (aufsichts-) rechtliche Anforderungen zu beachten.	x	x	x	x	x
ID.09.02.06-01	Wechselt ein Mitarbeiter in eine andere Organisationseinheit und führt dort andere fachliche Aufgaben aus, so sind seine Zugriffsberechtigungen unverzüglich anzupassen. Nicht mehr benötigte Berechtigungen sind zu entziehen.	x		x	x	x
ID.09.02.06-02	Verlässt ein Mitarbeiter das Unternehmen sind seine Zugriffsberechtigungen unverzüglich zu entziehen und seine Benutzerkennungen unverzüglich dauerhaft zu sperren.	x	x	x	x	x
ID.09.03.01-01	Für die Verwendung von Passwörtern sind Vorgaben festgelegt, insbesondere zu den Themen Passwortlänge, Passwortkomplexität und Passwortänderungsintervall. Passwörter sind durch den Benutzer geheim zu halten und sind nicht an Dritte weiterzugeben. Die Regelung muss Bestandteil der schriftlich fixierten Ordnung sein.	x	x	x		x
ID.09.04.01-01	Rollen, Benutzergruppen und Benutzern werden immer nur die minimal erforderlichen Zugriffsrechte eingeräumt, um ihre fachlichen Aufgaben zu erfüllen („Need-To-Know Prinzip“). Es gilt der Grundsatz der minimalen, bedarfsgerechten Rechtevergabe.	x	x	x	x	x

ID.09.04.01-02	Die Identität eines Benutzers ist durch eine geeignete Authentifizierung festzustellen. Die Authentifizierungsmechanismen sind auf Basis der Risikoexposition zu implementieren.	x	x	x	x	x
ID.09.04.02-01	Bei erfolglosen Anmeldeversuchen ist nicht erkennbar, ob der eingegebene Benutzername oder das eingegebene Passwort (oder beides) falsch ist.	x	x	x	x	x
ID.09.04.02-02	Bei der Eingabe werden Authentifizierungsinformationen wie Passwörter, PIN etc. grundsätzlich nicht im Klartext angezeigt.	x	x	x		x
ID.09.04.02-03	In Abhängigkeit von der Kritikalität der Daten und der Exponiertheit des Systems sind zusätzliche geeignete Maßnahmen (bspw. temporäre/vollständige Sperrung des Zugriffs oder Löschung der Daten) zu definieren, die nach einer festgelegten Anzahl fehlerhafter Anmeldeversuche vollzogen werden.	x	x	x		x
ID.09.04.02-04	Authentifizierungsinformationen sind bei Übertragung durch kryptographische Maßnahmen zu schützen.	x	x	x		x
ID.09.04.02-05	Die folgenden Ereignisse sind für alle Benutzerkonten risikoorientiert zu protokollieren: • Erfolgreiche und fehlgeschlagene Anmeldeversuche • Passwortrücksetzungen • Sperren und Entsperren eines Benutzerkontos • Anlegen und Löschen eines Benutzerkontos • Vergabe, Änderung oder Entzug von Zugriffsberechtigungen	x		x		x
ID.09.04.02-06	Auf den Systemen ist ein Session Time Out zu konfigurieren, so dass innerhalb eines definierten Zeitraums ein automatisches Log-Off (oder Sperrung des Bildschirms) erfolgt. Inaktive Sessions müssen nach Ablauf des definierten Zeitraums terminiert werden.	x		x		x
ID.09.04.03-01	Standardkennungen und voreingestellte Default-Passwörter sind vor der erstmaligen Produktivsetzung eines IT-Assets zu ändern.	x		x		x
ID.09.04.04-01	Zugriffe, die die sicherheitsrelevante Konfiguration eines IT-Asset verändern, werden nur von administrativen Benutzerkonten ausgeführt. Die Zugriffe werden protokolliert.	x		x		x
ID.09.04.04-02	Die Notwendigkeit der Benutzung privilegierter Berechtigungen wird nachvollziehbar dokumentiert.	x		x	x	x
ID.09.04.05-01	Quelltext-Repositories sind mit einer Zugriffskontrolle versehen.		x			x
10 Kryptographie (ID.10 Cryptography)						
ID.10.01.01-01	Es existiert eine Richtlinie zur Verwendung von kryptographischen Verfahren.	x		x		x
ID.10.01.01-02	Für administrative Tätigkeiten ist mindestens auf Übertragungsebene (Netzwerk) ein kryptographisches Verfahren anzuwenden. Je nach Art der Tätigkeit kann die Verschlüsselung auch auf höheren Ebenen (Anwendungsebene) erfolgen.	x		x		x
ID.10.01.02-01	Bei der Verwendung von PKI-Zertifikaten haben die betroffenen IT-Assets die Vertrauenswürdigkeit eines Zertifikats zu prüfen	x		x		x
ID.10.01.02-02	Durch den Supplier sind PKI-Zertifikate, die nicht mehr korrekt sind oder bei denen der private Schlüssel abhandengekommen ist bzw. kompromittiert wurde, unverzüglich (max. innerhalb von 72 Stunden) nach Meldung zu sperren.	x		x		x
ID.10.01.02-03	Mit Ausnahme von CA-Zertifikaten haben PKI-Zertifikate im Produktionsumfeld einen Gültigkeitszeitraum von 3 Jahren nicht zu überschreiten.	x		x		x
ID.10.01.02-04	PKI-Zertifikate sind rechtzeitig vor Sperrung oder Ablauf des Gültigkeitszeitraums durch ein neues Zertifikat zu ersetzen. Bei der Erneuerung von PKI-Zertifikaten ist ein neues Schlüsselpaar zu verwenden.	x		x		x
ID.10.01.02-05	Die Verwendung von Wildcard-Zertifikaten (bspw. CN=*.dzbank.de) ist grundsätzlich nicht erlaubt und Bedarf der expliziten Freigabe durch den IT-Sicherheitsbeauftragten (ISO).	x		x		x
ID.10.01.02-06	Bei Betrieb einer eigenen Certification Authority (CA) ist der Zugriff auf die CA zu protokollieren.	x		x		x
ID.10.01.02-07	Bei Einsatz symmetrischer und asymmetrischer (nicht zertifikatsbasiert) Verschlüsselungsverfahren im Produktionsumfeld ist regelmäßig ein Tausch des Schlüsselmaterials vorzusehen.	x		x		x
11 Physische und umgebungsbezogene Sicherheit (ID.11 Physical and environmental security)						
ID.11.01.01-01	Physische Werte (Gebäude, Infrastrukturen) sind risikoorientiert in Sicherheitszonen zu unterteilen. Die definierten Sicherheitszonen sind zu dokumentieren.	x				x
ID.11.01.02-01	Für den physischen Zutritt zu den Sicherheitszonen sind risikoorientiert Maßnahmen zur Zutrittssteuerung definiert.	x				x

ID.11.01.02-02	Der Eintritt und Austritt aus Hochsicherheitsbereichen, in denen die Infrastruktur für produktiv genutzte IT-Assets (Rechenzentren, Serverräume) untergebracht ist, wird protokolliert.	x				x
ID.11.01.03-01	Physischer Schutz für Büros, Räume und Einrichtungen muss risikoorientiert unter Berücksichtigung der Sicherheitszone geplant und umgesetzt werden.	x				x
ID.11.01.04-01	Es sind risikoorientiert physische Schutzmaßnahmen vor externen und umweltbedingten Bedrohungen definiert und umgesetzt, um Schäden zu verhindern bzw. das Schadensausmaß zu verringern.	x				x
ID.11.01.05-01	Der Supplier hat Maßnahmen zu definieren, die bei der Arbeit in Hochsicherheitsbereichen zu berücksichtigen sind.	x				x
ID.11.01.06-01	Öffentliche Zugangspunkte wie Anlieferungs- und Ladezonen an denen unbefugte Personen den Standort betreten können, müssen kontrolliert und, sofern möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unerlaubten Zutritt zu verhindern.	x				x
ID.11.02.01-01	Bei der Auswahl des Standorts und der Lage physischer Werte (Ist-Zustand) wird eine Risikoabwägung unter Berücksichtigung von Umweltbedrohungen sowie unberechtigten Zutritten vorgenommen. Die Ergebnisse dieser Risikoabwägung sind dokumentiert.	x				x
ID.11.02.02-01	IT-Assets sind durch präventive Maßnahmen vor den Auswirkungen eines Ausfalls der zum Betrieb benötigten Services (z. B. Stromversorgung) geschützt.	x				x
ID.11.02.03-01	Strom- und Netzwerkkabel werden in Hochsicherheitsbereichen auf voneinander getrennten Trassen verlegt. Die Verlegung von Strom- und Netzwerkkabel im öffentlichen Bereich oder Außenbereich ist zu vermeiden. Die Verlegung von Strom- oder Netzwerkkabeln im öffentlichen Bereich oder Außenbereich ist durch zusätzliche Maßnahmen zu schützen, aber generell zu vermeiden.	x				x
ID.11.02.04-01	Eingesetzte physische Werte und Services werden gemäß Herstellerangabe regelmäßig gewartet.	x				x
ID.11.02.05-01	Geräte und Informationen dürfen nicht ohne Genehmigung den Standort verlassen, ausgenommen hiervon sind mobile Endgeräte	x				x
ID.11.02.06-01	Endgeräte sind bei der Nutzung in öffentlichen Bereichen risikoorientiert durch physische Sicherheitsmaßnahmen vor Entwendung und unerwünschter Einsicht zu schützen.	x		x	x	x
ID.11.02.07-01	Bei Entsorgung oder vor Wiederverwendung von physischen Werten, die Datenträger enthalten, sind die Anforderungen zur Löschung zu berücksichtigen. Datenschutz Hinweis*: Der Supplier speichert personenbezogene Daten ausschließlich auf löschfähigen Systemen. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x				x
ID.11.02.08-01	Unbeaufsichtigte IT-Systeme und Informationen sind durch geeignete Maßnahmen zu schützen, beispielsweise durch Aktivieren eines passwortgeschützten Bildschirmschoners.	x		x	x	x
ID.11.02.09-01	Der Grundsatz des aufgeräumten Schreibtisches für Papiere und Wechselmedien sowie des gesperrten Bildschirms für informationsverarbeitende Einrichtungen wird angewendet (Clear Desk und Clear Screen).	x		x	x	x
12 Betriebssicherheit (ID.12 Operations security)						
ID.12.01.01-01	Für die beim Supplier produktiv eingesetzten IT-Assets existiert eine Verfahrensdokumentation.	x				x
ID.12.01.02-01	Für Änderungen an den produktiv genutzten IT-Assets ist ein formaler Change Management Prozess zu definieren.	x		x	x	x
ID.12.01.03-01	Die vom Supplier produktiv eingesetzten IT-Assets sind hinsichtlich Auslastung und Performance risikoorientiert zu überwachen. Dazu sind Schwellwerte zu definieren, die frühzeitig Anpassungen an den eingesetzten Ressourcen ermöglichen.	x				x
ID.12.01.04-01	Entwicklungs-, Test- und Produktivumgebungen von IT-Assets sind voneinander zu trennen. Eine klare Trennung zu möglichen anderen Kunden des Suppliers muss vorhanden sein (Mandantentrennung).	x				x
ID.12.02.01-01	Auf Betriebssystemen ist ein Virenschutz installiert und die Virensignaturen sind stets auf dem aktuellen Stand zu halten. Die Aktualisierungszeiträume der Signaturen sind risikoorientiert festzulegen.	x	x	x	x	x
ID.12.02.01-02	Eingehende Daten aus Netzwerken außerhalb des Suppliers sind unabhängig von der clientseitigen Anti-Virensoftware durch zusätzliche Maßnahmen auf Schadsoftware zu prüfen.	x	x	x	x	x

ID.12.03.01-01	Es existieren dokumentierte Verfahren, die die Wiederherstellung eines IT-Asset ermöglichen. Dabei sind die sich aus Business Impact Analysen ergebenden Anforderungen zu reflektieren.	x		x	x	x
ID.12.04.01-01	Es sind Vorgaben zur sicherheitsrelevanten Ereignisprotokollierung definiert. Es muss ein Konzept (Logging-Konzept) vorhanden sein, das die grundlegenden Logging-Mechanismen über alle (im Auftrag der UIT / AFS) zu betreibende Systeme enthält. Das Konzept muss Informationen über Art der Log Files, Speicherort und Speicherzeit, Zugriffsregelungen und Schutzmechanismen enthalten. Es ist ein Prozess zu etablieren, der sicherstellt, dass die aufgezeichneten Protokolldaten untersucht werden.	x		x	x	x
ID.12.04.01-02	Es ist eine Ereignisprotokollierung für IT-Assets implementiert.	x	x	x		x
ID.12.04.01-03	Es sind relevante Security Events definiert, die in das Security Monitoring und Alerting einfließen.	x		x	x	x
ID.12.04.01-04	Security Events sind risikoorientiert möglichst zeitnah auf einem dedizierten, geschützten Log-Server zu erfassen und zu überwachen (Security Event Monitoring).	x		x	x	x
ID.12.04.01-05	Bei der Aufbewahrung sicherheitsrelevanter Log-Daten sind gesetzliche sowie. regulatorische Anforderungen und Fristen zu beachten.	x		x	x	x
ID.12.04.01-06	Sicherheitsrelevante Log-Dateien, die auf dolose Handlungen Interner hinweisen, werden von einer Organisationseinheit überwacht, die unabhängig von der operativen Einheit ist, die das IT-Asset betreibt.	x		x	x	x
ID.12.04.02-01	Sicherheitsrelevante Log-Daten sind vor Manipulation zu schützen. Die Korrektheit der Protokolldaten muss nachweislich gewährleistet sein. Es muss sichergestellt sein, dass die Daten nicht kompromittiert wurden.	x	x	x	x	x
ID.12.04.03-01	Privilegierte Aktivitäten sind zu protokollieren.	x	x	x	x	x
ID.12.04.04-01	Die Zeitgebung (Uhrzeit) aller IT-Assets des Suppliers ist mit einem definierten, einheitlichen Zeitserver zu synchronisieren. Dabei erfolgt eine Plausibilitätsprüfung der zu übernehmenden Zeitinformation.	x				x
ID.12.05.01-01	Es sind Verfahren zur Steuerung von Software-Installationen definiert.	x		x	x	x
ID.12.06.01-01	Schwachstellen (Sicherheitslücken) sind durch den Supplier im Rahmen definierter Verfahren zu behandeln.	x		x	x	x
ID.12.06.01-02	Sicherheitsrelevante Patches und Updates sind zeitnah nach Erscheinen auf ihre Relevanz hin zu prüfen sowie deren Einspielung zu planen und umzusetzen. Dieser Vorgang ist zu dokumentieren.	x	x	x	x	x
ID.12.06.01-03	Für alle aus dem Internet erreichbaren IP Adressen, die auf eine Domain des Suppliers registriert sind bzw. zum IP-Adressraum des Suppliers gehören, ist ein monatlicher, automatisierter Schwachstellenscan durchzuführen.	x	x	x	x	x
ID.12.06.01-04	IT-Assets, die Dienste im Internet bereitstellen, sind in Abhängigkeit ihres Schutzbedarfs vor der Produktivsetzung und im laufenden Betrieb risikoorientiert regelmäßig einem Penetrationstest zu unterziehen.	x		x	x	x
ID.12.06.02-01	Bei dem Supplier sind Vorgaben für die Software Installation durch Benutzer zu definieren.	x			x	x
ID.12.07.01-01	Auditanforderungen und -tätigkeiten, welche eine Überprüfung betrieblicher Systems beinhalten, werden sorgfältig geplant und vereinbart, um Störungen der Geschäftsprozesse zu minimieren.	x				x
13 Kommunikationssicherheit (ID.13 Communications security)						
ID.13.01.01-01	Bei dem Supplier sind Rollen, Verantwortlichkeiten und Vorgehensweisen für die Verwaltung der IT-Assets der Kategorie Network-Management festgelegt und dokumentiert.	x				x
ID.13.01.01-02	Virtualisierte IT-Assets, die auf Basis des Schutzbedarfs, der Exponiertheit oder Anforderungen zur Trennung von Entwicklungs-, Test- und Produktivumgebungen in unterschiedlichen Netzwerkzonen betrieben werden, sind im Netzwerk zu separieren.	x				x
ID.13.01.01-03	Ein- und ausgehende Verbindungen am Übergang zwischen dem Netzwerk des Suppliers und anderen Netzwerken haben über bekannte und dokumentierte Gateways zustande zukommen.	x				x
ID.13.01.01-04	Das Routing von Daten innerhalb und an den Übergängen des Supplier-eigenen Netzwerks ist nur über Netzwerkkomponenten durchzuführen, die der operativen Kontrolle einer zentralen Organisationseinheit der Supplier oder eines durch die Organisation beauftragten Dienstleisters unterliegen.	x				x
ID.13.01.02-01	Die Kommunikation zwischen Netzwerkzonen (physisch, logisch) ist risikoorientiert auf ein notwendiges Minimum zu beschränken.	x				x

ID.13.01.02-02	Drahtlose Netzwerke (WLANs) sind aufgrund der schlecht definierbaren physikalischen Grenzen in separaten Netzwerkzonen zu betreiben.	x				x
ID.13.01.02-03	Es sind angemessene Mechanismen für die Steuerung des Zugriffs auf vertrauenswürdige Netzwerkzonen zu etablieren.	x				x
ID.13.01.02-04	Für die Authentifizierung und Verschlüsselung zur Netzwerkzugriffssteuerung sind angemessene Technologien und Standards einzusetzen.	x				x
ID.13.01.03-01	Es sind Gruppen von Informationsdiensten, Benutzern und Informationssystemen in Netzwerken voneinander zu trennen (Netzwerkzonierung).	x				x
ID.13.01.04-01	Der externe Zugriff auf das Netzwerk der Organisation ist grundsätzlich nur mit von der Organisation freigegebenen Remote Access Lösungen über gesicherte Kommunikationswege durchzuführen.	x				x
ID.13.01.04-02	Für den externen Zugriff auf das Netzwerk der Supplier ist eine erfolgreiche Autorisierung und Authentifizierung notwendig. Bei Remote Access Verbindungen aus dem Internet (öffentliche Netzwerke) ist eine Zwei-Faktor Authentifizierung zu verwenden.	x				x
ID.13.02.01-01	Bei dem Supplier sind risikoorientiert Maßnahmen definiert und etabliert, mit denen die Datenübertragung über alle Arten von Kommunikationseinrichtungen geschützt wird	x				x
ID.13.02.02-01	Bei dem Supplier existieren risikoorientiert Vereinbarungen für die Übertragung von geschäftlichen Informationen zwischen dem Supplier und externen Dritten.	x				x
ID.13.02.03-01	IT-Assets haben risikoorientiert die Identität der mit ihnen kommunizierenden IT-Assets zu verifizieren.	x				x
14 Anschaffung, Entwicklung und Instandhalten von Systemen (ID.14 System acquisition, development and maintenance)						
ID.14.01.01-01	Anforderungen zur Informationssicherheit sind als nicht-fachliche Anforderungen im Rahmen der Planung und (Weiter-) Entwicklung von IT-Assets strukturiert zu erheben und mit geeigneten Maß-nahmen zu adressieren. Dabei sind bei der Planung und (Weiter-) Entwicklung von Anwendungen (ODV) auch die zum Betrieb notwendigen IT-Assets zu berücksichtigen (Anwendung in Laufzeitumgebung). Datenschutz Hinweis*; Der Supplier hat die Grundsätze "Privacy by Design" und "Privacy by Default" implementiert. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x		x	x	x
ID.14.01.01-02	Bei der (Weiter-) Entwicklung eines IT-Assets ist der Schutzbedarf des jeweiligen IT-Assets zu verifizieren und unter Einbindung der definierten dezentralen Rolle (Business Information Security Officer (BISO)) zu definieren bzw. zu verifizieren.				x	x
ID.14.01.01-03	Bei der Einführung neuer Technologien für IT-Assets und damit verbundene Änderungen in der IT-Architektur des Suppliers wird der IT-Sicherheitsbeauftragter (CISO) eingebunden. Dabei ist der Grad der Einbindung risikoorientiert abzuwägen. Eine fachliche Einbindung und Mitzeichnung wird mindestens bei Einführung sicherheitsgebender Funktionen notwendig sichergestellt.	x		x	x	x
ID.14.01.02-01	Werden IT-Assets der Supplier an ein anderes als das organisationseigene Netzwerk angebunden, so ist die Verbindung mehrstufig und unter Einsatz von Paket- und Content-Filter zu schützen.	x				x
ID.14.01.03-01	Werden Information Assets als Transaktionen zwischen mehreren beteiligten IT-Assets ausgetauscht, so sind risikoorientiert Maßnahmen zum Schutz der Information Assets zu definieren. sodass eine unvollständige Übertragung, Fehlleitung, unbefugte Offenlegung, unbefugte Vervielfältigung oder unbefugte Wiederholung von Nachrichten verhindert wird.	x	x	x	x	x
ID.14.01.04-01	Werden Information Assets als sogenannte 'Data at Rest' persistiert, so sind risikoorientiert Maßnahmen zum Schutz der Information Assets zu definieren, sodass eine unbefugte Offenlegung oder Veränderung verhindert wird.	x				x
ID.14.02.01-01	Bei dem Supplier existieren Richtlinien für die (Software-) Entwicklung von Anwendungen (ODV und IDV).		x			x
ID.14.02.02-01	Änderungen an Konfigurationen von IT-Assets im Produktionsumfeld sind ausschließlich im Rahmen des definierten Changemanagement-Prozesses durchzuführen.	x		x	x	x

ID.14.02.03-01	Bei Änderungen an IT-Assets werden die mit den IT-Assets verbundenen Anwendungen (ODV) im Rahmen eines geregelten Prozesses risikoorientiert getestet, um negative Auswirkungen auf die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Anwendung auszuschließen. Dabei ist die definierte dezentrale Rolle (Business Information Security Officer (BISO)) einzubeziehen.	x				x
ID.14.02.03-02	Bei Änderungen an ODV-Anwendungen werden die darauf basierenden IDV-Anwendungen im Rahmen eines geregelten Prozesses risikoorientiert getestet, um negative Auswirkungen auf die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der IDV-Anwendung auszuschließen. Dabei ist die definierte dezentrale Rolle (Business Information Security Officer (BISO)) einzubeziehen.				x	x
ID.14.02.04-01	Bei der Paketierung von Komponenten eines IT-Assets werden Änderungen auf ein notwendiges Minimum beschränkt und im Rahmen formaler Prozesse nachvollziehbar dokumentiert.	x	x			x
ID.14.02.05-01	Es gelten folgende Mindestanforderungen: • Eine angemessene Validierung bzw. Plausibilisierung der Eingabedaten muss implementiert sein. • Die korrekte Funktion von Datenverarbeitungsprozessen muss gewährleistet sein. • Eine Validierung der Ausgabedaten muss implementiert sein.		x			x
ID.14.02.06-01	Im Rahmen der Entwicklung von Anwendungen (ODV) ist ein System für das Source Code Management (inkl. Versionskontrolle) einzusetzen.		x			x
ID.14.02.06-02	Im Rahmen der Entwicklung von Anwendungen (IDV) ist ein System zur Versionierung einzusetzen.		x			x
ID.14.02.06-03	Im Rahmen der Entwicklung von Anwendungen (ODV und IDV) ist verwendeter externer Source Code auf Schadcode zu prüfen. Die Vertrauenswürdigkeit der genutzten Quellen ist zu verifizieren.		x			x
ID.14.02.06-04	Im Rahmen der Anwendungsentwicklung sind risikoorientiert Vorkehrungen für individuell entwickelten Quellcode zu treffen, die nicht vorgesehene Änderungen an Anwendungen identifizieren können.		x			
ID.14.02.07-01	Bei ausgelagerter Entwicklung von IT-Assets überwacht der Supplier risikoorientiert die Tätigkeit der ausgegliederten Systementwicklung. Dabei ist die Überwachungstätigkeit durch einen Vertreter des Suppliers selbst durchzuführen. Art und Umfang der Überwachungstätigkeit richtet sich nach dem Schutzbedarf / der Exponiertheit des IT-Assets. Die Überwachung erfolgt in vergleichbarem Umfang zur internen Entwicklung.		x			x
ID.14.02.07-02	Bei ausgelagerter Entwicklung von Anwendungen (ODV) hat die Organisation schriftliche Vereinbarungen bzgl. der (Eigentums-) Rechte der Entwicklungsergebnisse zu treffen.		x			x
ID.14.02.08-01	Bei dem Supplier werden sicherheitsrelevante Aspekte im Rahmen der Entwicklung von Anwendungen (ODV) getestet.		x			x
ID.14.02.09-01	Vor der Überführung von IT-Assets in Produktion sind Sicherheitsfunktionen und deren Konfigurationen im Rahmen von Testverfahren zu prüfen.	x				x
ID.14.02.09-02	Die für den Test der Sicherheitsfunktion von IT-Asset genutzte (Test-) Umgebung ist vergleichbar der Produktionsumgebung konfiguriert.	x	x	x		x
ID.14.03.01-01	Werden im Entwicklungs- und Testumfeld (inkl. Integration) Produktionsdaten (unabhängig vom Alter der Daten) verwendet, so sind diese risikoorientiert auf Basis der Vertraulichkeitsanforderungen zu pseudonymisieren / anonymisieren oder mit denselben Mechanismen zu schützen wie im Pro-duktionsumfeld.		x			x
15 Lieferantenbeziehungen (ID.15 Supplier relationships)						
ID.15.01.01-01	Bevor eine externe Leistung in der Organisation produktiv eingesetzt wird, müssen Verträge inkl. relevanter Dokumente zur Informationssicherheit existieren und mit dem Dienstleister / Servicegeber schriftlich vereinbart sein Datenschutz Hinweis*: Es wurden ordnungsgemäße Verträge mit Sub-Dienstleistern, z.B. gem. Art. 28 DS-GVO geschlossen. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x		x	x	x

ID.15.01.01-02	Der Einkauf bzw. die Beauftragung von externen Leistungen hat unter Einbeziehung einer zentralen Stelle zu erfolgen. Neue Dienstleister sind in das Asset-Inventar aufzunehmen.	x		x	x	x
ID.15.01.02-01	Bei dem Supplier sind Verträge mit externen Dienstleistern zu vereinbaren, die Anforderungen zur Informationssicherheit berücksichtigen. Datenschutz Hinweis*: Im Falle der Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWR hat der Supplier geeignete Garantien zum Schutze dieser Daten implementiert. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x	x	x	x	x
ID.15.01.02-03	Bei Auslagerung des Betriebs oder der Entwicklung von IT-Assets ist die erbrachte Dienstleistung physisch oder logisch von den für andere Kunden erbrachten Dienstleistungen zu trennen.	x	x			x
ID.15.01.03-01	Vertragliche Vereinbarungen zur Informationssicherheit sind durch die Dienstleistern durchgängig auch bei an der Leistungserbringung beteiligten Dritten ("Unterauftragnehmer") zu berücksichtigen.	x		x	x	x
ID.15.02.01-01	Der Supplier überwacht (auditiert) risikoorientiert die Dienstleistungserbringung von Dienstleistern.	x		x	x	x
ID.15.02.02-01	Änderungen hinsichtlich der zu erbringenden Dienstleistungen / Services sind unter Einbeziehung einer zentralen Stelle zu steuern. Dabei sind risikoorientiert die Veränderungen an organisationseigenen Vorgaben (Richtlinien etc.) zu berücksichtigen und zeitnah im Vertragswerk zu berücksichtigen.	x		x	x	x
16 Handhabung von Informationssicherheitsvorfällen (ID.16 Information security incident management)						
ID.16.01.01-01	Bei dem Supplier sind Verantwortlichkeiten und Verfahren festzulegen, um schnell, effektiv und koordiniert auf Informationssicherheitsereignisse und -vorfälle zu reagieren. Die beteiligten Mitarbeiter der Supplier (z.B. Systemoperatoren) sind so vom Supplier zu schulen, dass der Prozess fehlerfrei angewendet werden kann. Datenschutz Hinweis*: Es ist ein angemessener und nachvollziehbarer Data Breach Prozess implementiert. (*Betrachtung erfolgt nicht durch ITSEC, sondern separat durch DSB)	x		x		x
ID.16.01.01-02	Bei dem Supplier ist ein Klassifizierungsschema zur Bewertung von Informationssicherheitsereignissen etabliert.	x		x		x
ID.16.01.02-01	Bei dem Supplier sind Informationssicherheitsereignisse gemäß den etablierten Verfahren zu melden. Es ist sicherzustellen, dass Sicherheitsvorfälle unverzüglich schriftlich der UIG mitgeteilt werden. Sofern ein Vorgang als schwerwiegend eingestuft wird, muss unverzüglich UIT-GRC (falls vertragsgebende Gesellschaft) und/oder UMH-BLC-KID-ISO (Information Security Office & IT-Compliance) in die weitere Bearbeitung eingebunden werden. Alle Folgeaktivitäten sind mit ihm im Vorfeld abzustimmen, sofern nicht Gefahr in Verzug ist.	x		x		x
ID.16.01.03-01	Mitarbeiter der Supplier und externe Parteien, die die IT-Assets der Supplier oder der UIG nutzen, sind dazu aufgefordert, jegliche beobachteten oder vermuteten Informationssicherheitslücken zu melden.	x		x	x	x
ID.16.01.04-01	Informationssicherheitsereignisse sind gemäß dem festgelegten Klassifizierungsschema zu untersuchen, und es ist darüber zu entschieden, ob sie als Informationssicherheitsvorfälle eingestuft werden.	x		x		x
ID.16.01.04-02	Für häufig / regelmäßig auftretende Informationssicherheitsereignisse hat der Supplier Standard-verfahren zu definieren und dokumentieren, die die Beeinflussung der Geschäftstätigkeit minimieren.	x		x		x
ID.16.01.05-01	Auf Informationssicherheitsvorfälle wird entsprechend den definierten Verfahren reagiert. Dabei ist eine Priorisierung auf Basis der Klassifizierung vorzunehmen. Dieser Vorgang ist zu dokumentieren.	x		x		x
ID.16.01.05-02	Aufgetretene Informationssicherheitsvorfälle werden auf Basis des Klassifizierungsschemas regelmäßig und anlassbezogen durch den IT-Sicherheitsbeauftragten (CISO) an den Vorstand / die Geschäftsführung berichtet.	x		x		x

ID.16.01.06-01	Bei dem Supplier sind die Aufzeichnungen zu Informationssicherheitsvorfällen regelmäßig zu analysieren und Maßnahmen abzuleiten.	x		x		x
ID.16.01.07-01	Bei dem Supplier sind Verfahren zur IT-forensischen Beweissicherung sowie die organisatorische Kompetenz zur Initiierung des Verfahrens zu etablieren.	x		x		x
17 Informationssicherheitsaspekte beim Business Continuity Management (ID.17 Information security aspects of business continuity management)						
ID.17.01.01-01	Die Anforderungen der Informationssicherheit werden durch den Supplier auch in Notfall-/Krisensituationen berücksichtigt.	x		x		x
ID.17.01.02-01	Der Supplier hat für die Informationssicherheit relevante Maßnahmen zur Notfallplanung festgelegt und dokumentiert.	x		x		x
ID.17.01.02-02	Bei dem Supplier werden Not- und Krisensituationen bei Abweichungen vom Normalbetrieb der Informationssicherheit die relevanten Ansprechpartner für sicherheitsgebende Funktionen eingebunden.	x		x		x
ID.17.01.03-01	Die festgelegten Maßnahmen zur Notfallplanung sind implementiert und werden regelmäßig auf Angemessenheit überprüft.	x		x		x
ID.17.01.03-02	Der Supplier bewertet alle eingetretenen Not-/Krisenfälle, sowie die getroffenen Entscheidungen und Maßnahmen werden zur Bewältigung in einer dokumentierten Nachschau bewertet und leitet daraus Verbesserungsmaßnahmen für die definierten Maßnahmen ab.	x		x		x
ID.17.02.01-01	IT-Assets und Supporting Assets sind auf Basis der Verfügbarkeitsanforderungen angemessen auszulegen.	x		x		x
18 Compliance (ID.18 Compliance)						
ID.18.01.01-01	Die für die Entwicklung und den Betrieb eines IT-Assets relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen sind zu dokumentieren.	x	x	x	x	x
ID.18.01.02-01	Bei Nutzung von extern entwickelter Standard- oder Individualsoftware sind die Vorgaben des Urheberrechtsgesetzes (UrhG) zu berücksichtigen. Der Supplier hat insbesondere die angemessene Lizensierung (Softwarelizenzen) zu prüfen. Bei Einsatz von Open-Source-Software sind die Lizenzbedingungen im gewerblichen Kontext zu prüfen, dies gilt auch im Kontext von Programmbibliotheken.	x	x	x		x
ID.18.01.02-02	Der Supplier hat verbindliche Regelungen zum Umgang mit urheberrechtlich geschützten Inhalten (insb. Bilder, Videos, Musik) definiert.	x	x	x	x	x
ID.18.01.03-01	Für geschäftliche Aufzeichnungen sind die jeweiligen Aufbewahrungsfristen im Rahmen eines Archivierungskonzeptes zu dokumentieren. Die Verfügbarkeit der Aufzeichnungen über die gesamte Aufbewahrungsdauer ist technisch zu gewährleisten.	x		x	x	x
ID.18.01.04-01	Der Supplier hat einen betrieblichen Beauftragten für den Datenschutz gem. Art. 37 Abs. 1 lit b,c DS-GVO bestellt. Die Umsetzung der Anforderungen zum Datenschutz wird durch den Datenschutzbeauftragten regelmäßig überwacht und bestätigt.	x		x	x	x
ID.18.01.04-02	Der Supplier hat alle Verfahren, in denen personenbezogene Daten verarbeitet werden, in einem Verfahrensverzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DS-GVO dokumentiert. Das Verfahrensverzeichnis enthält Aussagen zur Art und Umfang der technischen und organisatorischen Maßnahmen zum Schutz der Daten.			x	x	x
ID.18.01.05-01	Es erfolgt eine Prüfung und Freigabe hinsichtlich der regulatorischen Zulässigkeit des Einsatzes der kryptographischen Maßnahmen.	x		x		x
ID.18.01.05-02	Werden kryptographische Verfahren durch Supplier umgangen, so sind die dazu angewandten Methoden durch den IT-Sicherheitsbeauftragten (ISO) freizugeben.	x		x		x
ID.18.02.01-01	• Security Audits und Security Assessments sind regelmäßig, grundsätzlich jährlich durchzuführen. • Audits müssen durch unabhängige Dritte oder durch eine interne Organisationseinheit, die nicht durch die leistungserbringenden Einheiten weisungsgebunden ist, durchgeführt werden. • Umfang, Vorgehen und Ergebnisse von Audits sind ausführlich zu dokumentieren und ISO (UMH-BLC-KID-ISO (Information Security Office & IT-Compliance)/ISO-LUX) zur Verfügung zu stellen. • ISO (UMH-BLC-KID-ISO (Information Security Office & IT-Compliance)/ISO-LUX) muss das Recht eingeräumt werden, uneingeschränkt Audits durchzuführen	x		x	x	x

ID.18.02.02-01	Die Umsetzung der Anforderungen zur Informationssicherheit wird durch den IT-Sicherheitsbeauftragten, bzw. ISO (falls kein Dienstleisterverhältnis mit UIT) regelmäßig überwacht und bestätigt.	x	x	x		x
ID.18.02.03-01	IT-Assets des Suppliers werden risikoorientiert einer technischen Prüfung unterzogen. Die Prüfung erfolgt auf produktiven Systemen bzw. Systemen, die vergleichbar der Produktivsysteme konfiguriert sind.	x				x

8.5.2.2 Erweitertes Vorgehen zu den Anforderungen der Richtlinie 5069

Auf Anforderung von Auftraggeber wird alternativ zum vereinfachten Vorgehen gemäß Ziffer 8.5.2.1 das erweiterte Vorgehen gemäß dieser Ziffer 8.5.2.2 zwischen den Parteien angewendet.
Der Auftragnehmer erhält dazu vom Auftraggeber einen separat als Anlage bereitgestellten Anforderungskatalog (wird in Form der RL-5069-Compliance-Checkliste - nachfolgend kurz „Checkliste“ genannt, bereitgestellt). Die durch den Auftraggeber dem Auftragnehmer bereitgestellte Checkliste ist vom Auftragnehmer als Selfassessment erstmalig auszufüllen und dem Auftraggeber ausgefüllt bereitzustellen.
Die Checkliste stellt die Gesamtschau aller Anforderungen (im Folgenden auch „Kontrollen“ genannt) dar, die abhängig von dem Leistungsbild und dem Kontext des Einsatzbereiches des Auftragnehmers Relevanz besitzen können. Die Konfektionierung der Checkliste erfolgt dabei über die folgenden Leistungsbilder: Infrastruktur-Betrieb, Anwendungsentwicklung/-Implementierung, technische Anwendungsbetreuung, fachliche Anwendungsbetreuung und SaaS. Die für den Auftragnehmer relevanten Kontrollen (Konfektionierung) inklusive der zugehörigen Konkretisierungen (diese sind ebenfalls in der Checkliste dokumentiert) werden zwischen den Parteien abgestimmt, vertraglich vereinbart und sind durch den Auftragnehmer einzuhalten.
Die in der Checkliste dokumentierten Konkretisierungen verweisen zum Teil auf weiterführende detaillierende Security-Standards. Diese Security-Standards befinden sich als eingebettete Dokumente im Reiter „Security-Standards“ der Checkliste. Sofern in einer relevanten Kontrolle bzw. in der Konkretisierung der relevanten Kontrolle auf einen Security-Standard verwiesen wird, wird dieser Teil der vertraglichen Vereinbarung zwischen den Parteien und ist durch den Auftragnehmer ebenfalls einzuhalten.
Nach der initialen vertraglichen Vereinbarung der Checkliste erfolgt jährlich ein Review der Checkliste. Im Rahmen des Reviews ist die Checkliste wiederholt durch den Auftragnehmer auszufüllen und dem Auftraggeber ausgefüllt bereitzustellen. Bei Änderungen bzw. Anpassungen der Checkliste sowie der zugehörigen Konkretisierungen wird diese aktualisiert mit einem Vertragschange, z.B. im Rahmen eines Nachtrags zum bestehenden Vertrag, vereinbart.
Solange und soweit diese Checkliste zwischen den Parteien nicht vertraglich vereinbart ist, sind die Anforderungen gemäß Ziffer 8.5.2.1 durch den Auftragnehmer einzuhalten.

8.5.3 Regelungen für die Handhabung von Informationen in Abhängigkeit der Vertraulichkeit

Nr.	C0	C1	C2	C3	Regelung
Weitergabe / Verteilerkreise					
1-1	X				Das Dokument darf an jeden verteilt werden.
1-2		X			Das Dokument darf ohne weitere Genehmigung an Mitarbeiter der UIG weitergegeben werden, sofern dies zu deren Aufgabenerfüllung erforderlich ist. An Dritte ist eine Weitergabe nur dann erlaubt, wenn das Dokument ausdrücklich für sie bestimmt ist.
1-3			X	X	Bei Weitergabe ist eine Kennzeichnung der Dokumente erforderlich.

Nr.	C0	C1	C2	C3	Regelung
1-4			X		Das Dokument darf nur innerhalb eines eingeschränkten und definierten Nutzerkreises verteilt werden. Der Verteilerkreis muss nicht durch Nennung einzelner Namen bestimmt sein, eine Definition beispielsweise anhand von Abteilungs- oder Projektbezeichnungen ist ausreichend.
1-5				X	Das Dokument darf nur an einzelne, namentlich ausgewiesene Personen (UIG und Kunden / Lieferanten) verteilt werden.
Gesprochenes Wort					
2-1	X	X			Informationen dürfen ortsunabhängig mündlich ausgetauscht werden.
2-2			X		Der mündliche Informationsaustausch ist in öffentlichen Bereichen nur unter Wahrung besonderer Sorgfalt gestattet, also wenn ein zufälliges Mithören Dritter ausgeschlossen werden kann.
2-3				X	Der mündliche Informationsaustausch ist nur in vertrauenswürdigen geschlossenen Räumen gestattet. Besondere Sorgfalt ist zu wahren, um ein Belauschen (z.B. an der geschlossenen Tür) zu verhindern.
Elektronische Speicherung					
3-1			X		Eine Speicherung ist nur in zugriffsbeschränkten Verzeichnissen erlaubt.
3-2				X	Eine Speicherung ist nur in zugriffsbeschränkten Verzeichnissen erlaubt und muss zusätzlich verschlüsselt erfolgen.
3-3	X	X	X		Eine Speicherung bei Cloud-Anbietern ist zulässig. Sofern personenbezogene Daten gespeichert werden, muss die Datenhaltung grundsätzlich in Europa erfolgen.
3-4				X	Eine Speicherung bei Cloud-Anbietern ist zulässig, sofern die Daten durch die Cloud-Lösung oder auf Anwendungsebene mit vom Anbieter unabhängigen Schlüsseln verschlüsselt werden. Sofern personenbezogene Daten gespeichert werden, muss die Daten-haltung grundsätzlich in Europa erfolgen.
3-5	X	X			Keine besonderen Anforderungen.
Ausdrucke					
4-1			X	X	Nach Möglichkeit ist der „FollowMe-Printing“ oder ggf. „Private Printing“- / „Vertraulich Drucken“- Modus der zentralen Etagendrucker zu verwenden
4-2				X	Ein Ausdruck und/oder das Anfertigen einer Kopie sind nur nach Genehmigung durch den Data Owner / Autor erlaubt.
4-3	X	X			Keine besonderen Anforderungen.
Aufbewahrung von Dokumenten					
5-1			X	X	Der Zugriff auf Ablagen für Dokumente ist auf den Kreis der Adressaten einzuschränken.

Nr.	C0	C1	C2	C3	Regelung
5-2			X	X	Ausdrucke dürfen nicht unbeaufsichtigt z.B. in Druckern oder auf Schreibtischen liegen und müssen eingeschlossen aufbewahrt werden (Clear Desk Policy).
5-3			X		Die unbeaufsichtigte Aufbewahrung muss innerhalb der UIG-Gebäude in einem abgeschlossenen Schrank erfolgen.
5-5	X	X			Keine besonderen Anforderungen.
Außerhausverbringung / Arbeiten unterwegs					
6-1		X	X	X	Die Mitnahme von Dokumenten außer Haus ist auf ein Minimum zu beschränken.
6-2				X	Die Außerhausverbringung ist nur nach Genehmigung durch den BISO (Data Owner) / Autor erlaubt.
6-3		X			Ein Lesen/Bearbeiten von Dokumenten im öffentlichen Bereich (insbesondere öffentliche Verkehrsmittel) ist insofern erlaubt, als ein hinreichender Sichtschutz gewährleistet ist.
6-4			X	X	Dokumente dürfen in der Öffentlichkeit nur gelesen/bearbeitet werden, sofern eine Einsichtnahme unberechtigter Dritte verhindert werden kann.
6-5			X	X	Papierdokumente dürfen nicht in der Öffentlichkeit unbeaufsichtigt gelassen werden.
6-6				X	Die unbeaufsichtigte Aufbewahrung muss analog der Aufbewahrung innerhalb der UIG-Bürogebäude erfolgen. Bei Reisen sollten die Unterlagen nie unbeaufsichtigt sein.

Nr.	C0	C1	C2	C3	Regelung
Transport / Übermittlung					
7-1			X		Die elektronische Übertragung von Dokumenten an externe Adressen muss grundsätzlich verschlüsselt erfolgen. Eine Transportverschlüsselung ist mindestens vorzusehen, Alternativ die Verschlüsselung der Daten selbst (Siehe hierzu RL-5119 IT-Sicherheitsrichtlinie, Kapitel „Regelungen für den Einsatz von Kryptographie (Verschlüsselung)“.).
7-2				X	Die elektronische Übertragung von Dokumenten an externe Adressen muss verschlüsselt erfolgen. Siehe hierzu RL-5119 IT-Sicherheitsrichtlinie, Kapitel „Regelungen für den Einsatz von Kryptographie (Verschlüsselung)“.
7-3			X	X	Das Faxen von Dokumenten ist nur gestattet, wenn sichergestellt ist, dass außer dem Empfänger niemand Einsicht in die Dokumente nehmen kann (durch z.B. parallele Absprache am Telefon).
7-4			X	X	Bei Fax-Antworten und Rückfragen sind C2 / C3-vertrauliche Informationen zu schwärzen. Andernfalls ist Regel 7-4 anzuwenden.

Nr.	C0	C1	C2	C3	Regelung
7-7			X		Der Versand per Hauspost muss grundsätzlich in verschlossenen Umschlägen erfolgen.
7-8				X	Der Versand per Hauspost soll nur in Ausnahmefällen eine persönliche Übergabe ersetzen.
7-9				X	Der Außerhausversand von Papierdokumenten muss mittels Kurier erfolgen (Werttransport).
7-10	X	X			Keine besonderen Anforderungen.
Vernichtung					
8-1		X			Dokumente sind im Papierkorb zu entsorgen.
8-2			X	X	Dokumente müssen grundsätzlich in einem Shredder vernichtet oder in einem der abschließbaren Papiercontainer entsorgt werden.

Festlegung der Testfrequenz und Art des Tests in Abhängigkeit der Risikoklasse eines IT Assets

Risikoklasse	Testfrequenz	Art des Tests
Schutzklasse 3 – Hoch	12 Monate	Alternierend manuelle Pentests und automatisierte Scans
Schutzklasse 2 – Mittel	12 Monate	Alternierend manuelle Pentests und automatisierte Scans
Schutzklasse 0, 1 – Niedrig	36, 24 Monate	Automatisierte Scans und jedes dritte Jahr ein manueller Pentest

9 Zusammenstellung der Leitfragen

Zu Abschnitt3 ff	„Umweltschutz und Sicherheit für Fertigung, Montage & Leistung vor Ort“ *Wird der Lieferant bei einen Unternehmen der Union Investment Gruppe vor Ort tätig, fertigt oder montiert er Werke, die bei einen Unternehmen der Union Investment Gruppe vor Ort eingesetzt oder mit denen Mitarbeiter eines Unternehmen der Union Investment Gruppe in Berührung kommen werden?*
Zu Abschnitt4 ff	„Zutrittsberechtigungen und Zutrittskarten (Deutschland)“ *Werden Mitarbeiter des Lieferanten, bzw. Dienstleisters eigenbeweglich in den Gebäuden der Union Investment Gruppe, ausgenommen hiervon sind Besucher (diese sind über Besucherausweise abgedeckt) und Handwerker (individueller Zugang per Überwachung durch Stockwerksbeauftragten) sein?*
Zu Abschnitt 4.2 ff	„Netzwerkzugang, Zugriff auf IT-Systeme und Plattformen“ *Erhält bzw. verfügt der Lieferant bzw. seine Mitarbeiter über einen Zugang (z.B. auch per VPN-/RAS) zum Netzwerk der Union Investment Gruppe.?*
Zu Abschnitt 5.1ff	„Agenturleistungen, Kontakter, Produktioner“ *Wird der Lieferant / Agentur auch Steuerungsleistungen im Zusammenhang von Marketingproduktionen erbringen und hierbei im Namen und Auftrag des Auftraggebers Leistungen bei Drittunternehmen beauftragen und steuern?*
Zu Abschnitt 5.5 ff	„Erstellung von Materialien, Redaktionsarbeiten, Pflege von Social Media-Kanälen“ *Fertigt der Lieferant (Auftragnehmer) Materialien oder Content für die Union Investment an, oder tritt für und im Namen der Union Investment in der Öffentlichkeit auf?*
Zu Abschnitt 6.1 ff	„Entwicklung und Anpassung von Software und Softwarekomponenten“ *Wird durch den Auftragnehmer eine Anwendung entwickelt oder weiterentwickelt?*
Zu Abschnitt 6.2 ff	„Test-, Release- und Deployment Management“ *Werden durch den Auftragnehmer, in der Rolle als Hersteller, Dienstleister oder Provider, Anpassungen technischer und/oder fachlicher Art vorgenommen oder bereitgestellt, die wesentlichen Änderungen an produktiven IT-Systemen darstellen? Es gilt die regulatorischen Vorgaben MaRisk, InvMaRisk, BAIT und für rechnungsrelevante Systeme in der GoBS und FAIT1 zu beachten.*
Zu Abschnitt 7.1 ff	„Incident- und ServiceRequest-Management Prozess“ *Ist der Lieferant bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?*
Zu Abschnitt 7.2 ff	„Problem-Management“ *Ist der Lieferant bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?*
Zu Abschnitt 7.3 ff	„Change-Management“ *Ist der Lieferant bei seiner Leistungserbringung a) für das Funktionieren einer IT-Komponente (z.B. IT-Asset, Applikation etc.) gegenüber dem Auftraggeber verantwortlich oder b) auf eine solche Komponente angewiesen und c) verfügt dabei nicht über ein eigenes systemunterstütztes IT-Service Management, welches an die ITSM-Infrastruktur der UIG angeschlossen ist?*
Zu Abschnitt 8 ff	„IT-Sicherheitsstandards: Anforderungen an Supplier“ Erbringt der Lieferant bzw. *Dienstleister Leistungen in einem der folgenden Themenfelder, bzw. nimmt dort Rollen und Aufgaben wahr: Infrastruktur-Betrieb,*

Anwendungsentwicklung/-Implementierung, technische Anwendungsbetreuung, fachliche Anwendungsbetreuung oder sonstige Anwendungsbetreuung?