Bundesamt
für Sicherheit in der
Informationstechnik

# OPS.2.3 Nutzung von Outsourcing

## 1. Beschreibung

### 1.1. Einleitung

Beim Outsourcing lagern Institutionen (Nutzende von Outsourcing) Geschäftsprozesse oder Tätigkeiten ganz oder teilweise zu einem oder mehreren externen Dienstleistungsunternehmen (Anbietende von Outsourcing) aus. Diese sogenannten Anbietenden von Outsourcing betreiben im Rahmen des vereinbarten Outsourcing-Verhältnisses die Geschäftsprozesse oder Tätigkeiten nach festgelegten Kriterien. Allerdings verbleibt die Verantwortung aus Sicht der Informationssicherheit stets bei der auslagernden Institution.

Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten der Auftraggebenden oder in einer externen Betriebsstätte der Anbietenden von Outsourcing erbracht werden kann. Typische Beispiele des klassischen "IT-Outsourcings", worauf sich dieser Baustein bezieht, sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe konkretisiert wird, wie Hosting, Housing oder Colocation.

Ein Outsourcing-Verhältnis betrifft neben den ursprünglichen Nutzenden und Anbietenden von Outsourcing in vielen Fällen weitere, den Anbietenden von Outsourcing nachgelagerte, Sub-Dienstleistende. Werden Teile von Geschäftsprozessen oder Tätigkeiten von Anbietenden von Outsourcing weiter an Sub-Dienstleistende verlagert, so werden die von Nutzenden ausgelagerten Geschäftsprozesse oder Tätigkeiten weiter fragmentiert. Dies wirkt sich auf die Komplexität der Outsourcing-Kette aus, woraus eine schwindende Transparenz für die Nutzenden von Outsourcing folgt. Der Nachweis, dass die an die Anbietenden von Outsourcing gestellten Anforderungen erfüllt werden, erstreckt sich hierbei sowohl auf die Anbietenden von Outsourcing als auch auf die Sub-Dienstleistenden.

Zur besseren Verständlichkeit wird in diesem Baustein der Begriff "Prozess" stellvertretend für Geschäftsprozess, Tätigkeit oder Komponente verwendet, die ausgelagert wird.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Grundwerte der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit über den gesamten Lebenszyklus des Outsourcings durch die Nutzenden von Outsourcing sicherzustellen. Mit Outsourcing ist dabei das klassische "IT-Outsourcing" gemeint.

Die Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* sollen dazu beitragen, dass potenzielle Gefährdungen für den Geschäftsbetrieb erkannt, vorgebeugt und vermindert werden.

Risiken für eine Institution sollen hierdurch in einem für die Institution kontrollierbaren Rahmen bleiben. Dies kann durch mehr Transparenz und Steuerungsinstrumenten erreicht werden. Dazu wird die Institution in ihrer Planung, Durchführung und Kontrolle des Outsourcing-Prozesses über den gesamten Lebenszyklus hinsichtlich technischen und nicht-technischen Aspekten der Informationssicherheit unterstützt.

## 1.3. Abgrenzung und Modellierung

Der Baustein OPS.2.3 *Nutzung von Outsourcing* ist für jede oder jeden Anbietenden von Outsourcing aus Sicht des Nutzenden von Outsourcing einmal anzuwenden.

Dieser Baustein behandelt Gefährdungen und Sicherheitsanforderungen aus Sicht der Nutzenden von Outsourcing-Leistungen und beschränkt sich auf die Anforderungen des Schutzes von Informationen seitens der auslagernden Institution.

Dieser Baustein behandelt nicht die Übertragungswege zu Anbietenden von Outsourcing.

Ebenso wird die Nutzung von Cloud-Diensten nicht in diesem Baustein behandelt, hierzu ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.

Vom klassischen „IT-Outsourcing“ (wie dem Betrieb von Hard- und Software, Hosting, Housing usw.) abweichende Szenarien können mit dem Baustein OPS.2.3 *Nutzung von Outsourcing* mitunter nicht abschließend abgebildet werden und benötigen unter Umständen eine separate Risikoanalyse.

Als Sonderfall zählen Sicherheitsdienste, Reinigungskräfte, Wartungsdienste und Fremdpersonal, für die der Baustein OPS.2.3 *Nutzung von Outsourcing* nicht anzuwenden ist. Diese werden über die Anforderungen zu Sicherheitsdiensten, Reinigungskräften, Wartungsdiensten und Fremdpersonal in den Bausteinen ORP.1 *Organisation* und INF.1 *Allgemeines Gebäude* eingebunden.

Das Pendant zum Baustein OPS.2.3 *Nutzung von Outsourcing* bildet der Baustein OPS.3.2 *Anbieten von Outsourcing*, der das Outsourcing-Verhältnis aus der Sicht der Dienstleistenden behandelt. Zusammen bilden die beiden Bausteine ein ganzheitliches Bild des Outsourcing-Verhältnisses ab und sorgen mit ihren Anforderungen für ein grundlegendes sicheres Outsourcing-Vorhaben.

# 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.2.3 *Nutzung von Outsourcing* von besonderer Bedeutung.

## 2.1. Unzureichende Strategie für das Outsourcing

Eine unzureichende Strategie führt dazu, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Hierdurch wird die Informationssicherheit nicht angemessen in den einzelnen Phasen des Outsourcing-Lebenszyklus beachtet und somit kein ausreichendes Niveau der Informationssicherheit in der eigenen Institution sowie bei Anbietenden von Outsourcing angestrebt und umgesetzt. Dadurch können Prozesse beeinträchtigt, ausfallen und Informationen an unbefugte Dritte abfließen.

## 2.2. Gefahr des Outsourcings von institutionskritischen Prozessen

Prozesse, die aufgrund ihrer Kritikalität oder des Schutzbedarfs in der Institution verbleiben sollten, werden ausgelagert. Infolgedessen kann die Institution den Prozess, der für den ordentlichen Geschäftsbetrieb notwendig ist, nicht mehr angemessen kontrollieren und steuern. Wenn der Prozess ausfällt oder gestört wird, kann kein ordentlicher Geschäftsbetrieb sichergestellt werden. Darüber

hinaus gewinnen die Anbietenden von Outsourcing einen größeren Einfluss. Es droht den Nutzenden von Outsourcing ein Steuerungsverlust.

## 2.3. Abhängigkeit von Anbietenden von Outsourcing

Entscheidet sich eine Institution für Outsourcing, macht sie sich damit auch von Anbietenden von Outsourcing abhängig. Mit dieser Abhängigkeit kann Wissen verloren gehen und die ausgelagerten Prozesse können nicht mehr vollständig kontrolliert werden. Außerdem könnte der Schutzbedarf der ausgelagerten Geschäftsprozesse und Informationen unterschiedlich eingeschätzt werden. Dies kann dazu führen, dass für den Schutzbedarf entsprechend ungeeignete Sicherheitsmaßnahmen umgesetzt werden. Häufig lagern Institutionen gesamte Geschäftsprozesse an Anbietende von Outsourcing aus. Die Anbietenden von Outsourcing können dadurch die Geschäftsprozesse mit schutzbedürftigen Informationen, Ressourcen und IT-Systemen vollständig kontrollieren. Gleichzeitig nimmt das Wissen über diese Bereiche bei Nutzenden von Outsourcing ab. Als Folge ist es möglich, dass die Nutzenden von Outsourcing Defizite der Informationssicherheit nicht mehr bemerken. Diese Situation könnte von Anbietenden von Outsourcing ausgenutzt werden, z. B. indem sie drastisch die Preise erhöhen oder die Qualität der Dienstleistungen abnimmt.

## 2.4. Unzureichendes Niveau der Informationssicherheit beim Outsourcing

Ein unzureichendes Niveau an Informationssicherheit kann dazu führen, dass die Informationssicherheit in Outsourcing-Vorhaben nicht angemessen berücksichtigt wird. Die Folge ist, dass die Anbietenden von Outsourcing keinen oder einen nur unzureichenden Standard der Informationssicherheit für den Outsourcing-Prozess aufrechterhalten. Folglich entstehen Schwachstellen, von denen IT-gestützte Angriffe sowie Datenverluste ausgehen können. Darüber hinaus können für die Nutzenden von Outsourcing rechtliche Konsequenzen mit finanziellen Auswirkungen sowie Reputationsverluste entstehen.

## 2.5. Mangelhaftes Auslagerungsmanagement

Ein nicht vorhandenes oder nur teilweise umgesetztes Auslagerungsmanagement äußert sich dadurch, dass die laufenden ausgelagerten Prozesse unzureichend verwaltet werden. Dadurch verringert oder verliert sich die Transparenz über die ausgelagerten Prozesse. Hierdurch können Nutzende von Outsourcing die Anbietenden von Outsourcing nicht mehr kontrollieren und angemessen steuern. Die Nutzenden von Outsourcing können nicht mehr sicherstellen, dass die Anbietenden von Outsourcing in dem ausgelagerten Prozess die Informationssicherheit sorgfältig behandeln.

## 2.6. Unzulängliche vertragliche Regelungen mit Anbietenden von Outsourcing

Unzulängliche vertragliche Regelungen mit den Anbietenden von Outsourcing können zu Schwachstellen in der Informationssicherheit entlang des gesamten Outsourcing-Lebenszyklus führen. Die vertraglichen Regelungen definieren den gesamten Outsourcing-Prozess und stellen den Ausgangspunkt für Ansprüche der Nutzenden gegenüber den Anbietenden von Outsourcing dar. Aufgrund von unzulänglichen vertraglichen Regelungen mit den Anbietenden von Outsourcing können vielfältige und auch schwerwiegende Sicherheitsprobleme auftreten. Wenn Aufgaben, Leistungsparameter oder Aufwände ungenügend oder missverständlich beschrieben wurden, können möglicherweise aus Unkenntnis oder wegen fehlender Ressourcen Sicherheitsmaßnahmen nicht umgesetzt werden. Dies kann viele negative Auswirkungen nach sich ziehen, etwa, wenn regulatorische Anforderungen und Pflichten nicht erfüllt oder Auskunftspflichten und Gesetze nicht eingehalten werden. Wird bei der Vertragsgestaltung der Aspekt der Informationssicherheit nicht

berücksichtigt, so können Prozesse und Daten der Nutzenden von Outsourcing unzureichend abgesichert werden.

## 2.7. Ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten

Je nach Outsourcing-Vorhaben kann es erforderlich sein, dass die Mitarbeitenden von Anbietenden von Outsourcing Zutritts-, Zugangs- und Zugriffsrechte zu IT-Systemen, Informationen, Gebäuden oder Räumen der Nutzenden von Outsourcing benötigen. Diese Rechte können ungeeignet vergeben, verwaltet und kontrolliert werden, hierdurch können im Extremfall sogar unautorisiert Rechte vergeben werden. Außerdem kann der notwendige Schutz der Informationen der Nutzenden von Outsourcing nicht mehr gewährleistet werden. Beispielsweise ist es ein gravierendes Sicherheitsrisiko, unkontrolliert administrative Berechtigungen an Mitarbeitende von Anbietenden von Outsourcing zu vergeben. Diese könnten Berechtigungen ausnutzen und sensible Informationen kopieren oder manipulieren.

## 2.8. Kontroll- und Steuerverlust durch Weiterverlagerungen

Teile von Geschäftsprozessen oder Tätigkeiten werden von Anbietenden von Outsourcing unter Umständen vollständig oder partiell an Sub-Dienstleistende weitergegeben. Da durch die zusätzlichen Beteiligten der Outsourcing-Prozess komplexer wird, wird dieser für die Nutzenden von Outsourcing intransparenter. Durch diese fehlende Transparenz können die Nutzenden von Outsourcing die ausgelagerten Prozesse nicht mehr angemessen kontrollieren und steuern. Darüber hinaus können Anbietende von Outsourcing versäumen, dass von Nutzenden von Outsourcing geforderte Mindestniveau der Informationssicherheit vom Sub-Dienstleistenden einzufordern. Eine Folge ist, dass unter Umständen die vereinbarten informationstechnischen Sicherheitsaspekte von den Sub-Dienstleistenden nicht vollständig umgesetzt werden.

## 2.9. Fehlende und unzulängliche Instrumente zur Steuerung von Anbietenden von Outsourcing

Damit eine Institution prüfen kann, ob die ausgelagerten Prozesse von Anbietenden von Outsourcing ordnungsgemäß umgesetzt werden, benötigt sie neben entsprechenden Vereinbarungen auch die Instrumente dazu. Dies können beispielsweise qualitative und quantitative Leistungskennzahlen (KPIs) sein. Um auf Minder- und Schlechtleistung reagieren zu können, werden entsprechend festgelegte Leistungskennzahlen benötigt. Fehlende und unzulängliche Instrumente führen dazu, dass die Anbietenden von Outsourcing nicht adäquat kontrolliert und gesteuert werden können. Dadurch kann nicht mehr geprüft und nachvollzogen werden, ob die festgelegten Sicherheitsanforderungen eingehalten werden.

## 2.10. Unzulängliche Regelungen für eine geplante und ungeplante Beendigung eines Outsourcing-Verhältnisses

Ein Outsourcing-Verhältnis kann ordentlich gekündigt oder auch außerordentlich beendet werden. Hierbei können unzulängliche oder fehlende Regelungen dazu führen, dass Hardware, Daten und Zugänge nicht oder nicht ordnungsgemäß an die Nutzenden von Outsourcing übergeben bzw. übermittelt werden.

## 2.11. Unzureichendes Notfallkonzept

Im Falle einer Störung, eines Notfalls oder einer Krise kann ein unzureichendes Notfallmanagement dazu führen, dass die ausgelagerten Prozesse ausfallen. Dabei bereitet insbesondere eine unzureichende

Notfallvorsorge die Institution in ungenügendem Maße auf eine Not- oder Krisensituation vor. Eine effektive Notfallbewältigung kann auf dieser Grundlage nicht sichergestellt werden. Störungen, Not- und Krisensituationen können nicht kontrolliert werden und zu unmittelbaren wirtschaftlichen Auswirkungen führen. In diesem Fall ist nicht nur die eigene Institution, sondern auch alle angebundenen Institutionen, die in der Notfallvorsorge und Notfallbewältigung berücksichtigt werden müssen, betroffen. Kaskadeneffekte durch vor- und nachgelagerte Dienstleistende führen zu beträchtlichen Auswirkungen auf den Geschäftsbetrieb der Nutzenden von Outsourcing.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.2.3 *Nutzung von Outsourcing* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | IT-Betrieb |
| Weitere Zuständigkeiten | Fachverantwortliche, Beschaffungsstelle, Zentrale Verwaltung, Notfallbeauftragte, Personalabteilung |

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

## 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

### OPS.2.3.A1 Erstellung von Anforderungsprofilen für Prozesse (B) [Fachverantwortliche]

Falls keine Business-Impact-Analyse (BIA) vorhanden ist, MÜSSEN Anforderungsprofile in Form von Steckbriefen für die Prozesse angefertigt werden, die potenziell ausgelagert werden sollen. Diese Anforderungsprofile MÜSSEN die Funktion, verarbeite Daten, Schnittstellen sowie eine Bewertung der Informationssicherheit enthalten. Insbesondere MÜSSEN die Abhängigkeiten zwischen den Prozessen sowie zu untergeordneten Teilprozessen berücksichtigt werden. Die Anforderungsprofile MÜSSEN die Kritikalität des jeweiligen Prozesses für den ordentlichen Geschäftsbetrieb abbilden.

### OPS.2.3.A2 Verfolgung eines risikoorientierten Ansatzes im Auslagerungsmanagement (B)

Für Prozesse, die potenziell ausgelagert werden sollen, MUSS risikoorientiert betrachtet und entschieden werden, ob diese ausgelagert werden können. Für diese Bewertung SOLLTEN die Anforderungsprofile als Grundlage genutzt werden. Wenn der Prozess ausgelagert wird, SOLLTE das Resultat im Auslagerungsregister abgelegt werden. Um Änderungen an Prozessen oder der Gefährdungslage zu berücksichtigen, MÜSSEN in regelmäßigen Abständen sowie anlassbezogen die ausgelagerten Prozesse erneut risikoorientiert betrachtet werden.

## OPS.2.3.A3 Festlegung von Eignungsanforderungen an Anbietende von Outsourcing (B) [Fachverantwortliche, Institutionsleitung]

Interne Eignungsanforderungen an potenzielle Anbietende von Outsourcing MÜSSEN festgelegt werden. Diese Eignungsanforderungen MÜSSEN die erforderlichen Kompetenzen, um den Prozess aus Sicht der Informationssicherheit abzusichern, sowie die Reputation hinsichtlich der Vertrauenswürdigkeit und Zuverlässigkeit berücksichtigen. Diese Eignungsanforderungen SOLLTEN auf Basis der Unternehmensstrategie (siehe OPS.2.3.A8 *Erstellung einer Strategie für Outsourcing-Vorhaben*) erstellt werden. Es MUSS geprüft werden, ob potenzielle Interessenkonflikte vorliegen. Ferner SOLLTEN die Anbietenden von Outsourcing regelmäßig gegen die Eignungsanforderungen geprüft werden. Wenn die Anbietenden von Outsourcing nicht die Eignungsanforderungen erfüllen, SOLLTEN Handlungsmaßnahmen getroffen und in einem Maßnahmenkatalog festgehalten werden.

## OPS.2.3.A4 Grundanforderungen an Verträge mit Anbietenden von Outsourcing (B)

Einheitliche Grundanforderungen an Outsourcing-Verträge MÜSSEN entwickelt werden. Diese Grundanforderungen MÜSSEN Aspekte der Informationssicherheit, einen Zustimmungsvorbehalt bei Weiterverlagerungen sowie ein Recht auf Prüfung, Revision und Audit beinhalten. Bei der Entwicklung der Grundanforderungen SOLLTEN die Resultate der risikoorientierten Betrachtung sowie Eignungsanforderungen an Anbietende von Outsourcing mit einfließen. Mit den Anbietenden von Outsourcing SOLLTE eine Verschwiegenheitserklärung zum Schutz von sensiblen Daten vereinbart werden. Die Grundanforderungen MÜSSEN in Vereinbarungen und Verträgen einheitlich umgesetzt werden. Auf Basis der Grundanforderungen SOLLTE eine einheitliche Vertragsvorlage erstellt und für alle Outsourcing-Vorhaben genutzt werden.

## OPS.2.3.A5 Vereinbarung der Mandantenfähigkeit (B)

In einer Vereinbarung zur Mandantenfähigkeit mit den Anbietenden von Outsourcing MUSS sichergestellt werden, dass die Daten und Verarbeitungskontexte durch den Anbietenden von Outsourcing ausreichend sicher getrennt sind. In dieser Vereinbarung SOLLTE ein Mandantentrennungskonzept von den Anbietenden von Outsourcing gefordert werden. Das Mandantentrennungskonzept SOLLTE zwischen mandantenabhängigen und mandantenübergreifenden Daten und Objekten unterscheiden und darlegen, mit welchen Mechanismen die Anbietenden von Outsourcing trennen.

## OPS.2.3.A6 Festlegung von Sicherheitsanforderungen und Erstellung eines Sicherheitskonzeptes für das Outsourcing-Vorhaben (B)

Mit den Anbietenden von Outsourcing MUSS vertraglich vereinbart werden, dass IT-Grundschutz umgesetzt oder mindestens die Anforderungen aus den relevanten Bausteinen geeignet erfüllt werden. Darüber hinaus SOLLTE mit den Anbietenden von Outsourcing vereinbart werden, dass sie ein Managementsystem für Informationssicherheit (ISMS) etablieren. Die Nutzenden von Outsourcing MÜSSEN für jedes Outsourcing-Vorhaben ein Sicherheitskonzept basierend auf den sich aus dem IT-Grundschutz ergebenen Sicherheitsanforderungen erstellen. Dabei MUSS das Sicherheitskonzept der Nutzenden mit den Anbietenden von Outsourcing abgestimmt werden. Ebenso SOLLTE jeder Anbietende ein individuelles Sicherheitskonzept für das jeweilige Outsourcing-Vorhaben vorlegen. Das Sicherheitskonzept der Anbietenden von Outsourcing und dessen Umsetzung SOLLTE zu einem gesamten Sicherheitskonzept zusammengeführt werden. Wenn Risikoanalysen notwendig sind, MÜSSEN Vereinbarungen getroffen werden, wie die Risikoanalyse geprüft und gegebenenfalls in das eigene Risikomanagement überführt werden kann. Die Nutzenden von Outsourcing oder unabhängige Dritte MÜSSEN regelmäßig überprüfen, ob das Sicherheitskonzept wirksam ist.

### OPS.2.3.A7 Regelungen für eine geplante oder ungeplante Beendigung eines Outsourcing-Verhältnisses (B) [Fachverantwortliche, Institutionsleitung]

Für geplante sowie ungeplante Beendigungen des Outsourcing-Verhältnisses MÜSSEN Regelungen getroffen werden. Es MUSS festgelegt werden, wie alle Informationen, Daten und Hardware der Nutzenden vom Anbietenden von Outsourcing zurückgegeben werden. Hierbei MÜSSEN gesetzliche Vorgaben zur Aufbewahrung von Daten beachtet werden. Ferner SOLLTE überprüft werden, ob die Zugangs-, Zutritts- und Zugriffsrechte für die Anbietenden von Outsourcing mit der Beendigung des Outsourcing-Verhältnisses aufgehoben wurden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

### OPS.2.3.A8 Erstellung einer Strategie für Outsourcing-Vorhaben (S) [Institutionsleitung]

Eine Strategie für Outsourcing-Vorhaben SOLLTE erstellt und etabliert werden. In dieser Strategie SOLLTEN die Ziele, Chancen und Risiken der Outsourcing-Vorhaben beschrieben werden. Die Strategie SOLL der Institution einen Rahmen für die Anforderungsprofile, die Eignungsanforderung an Anbietende von Outsourcing sowie dem Auslagerungsmanagement vorgeben. Darüber hinaus SOLLTEN neben den wirtschaftlichen, technischen, organisatorischen und rechtlichen Rahmenbedingungen auch die relevanten Aspekte der Informationssicherheit berücksichtigt werden. Es SOLLTE eine Multi-Sourcing Strategie verfolgt werden, um Engpässe sowie Abhängigkeiten von Anbietenden von Outsourcing zu vermeiden. Die Nutzenden von Outsourcing SOLLTEN ausreichend Fähigkeiten, Kompetenzen sowie Ressourcen behalten, um einer Abhängigkeit gegenüber den Anbietenden von Outsourcing vorzubeugen.

### OPS.2.3.A9 Etablierung einer Richtlinie zur Auslagerung (S) [Institutionsleitung]

Auf Basis der Strategie für Outsourcing-Vorhaben SOLLTE eine Richtlinie für den Bezug von Outsourcing-Dienstleistungen erstellt und in der Institution etabliert werden. Diese SOLLTE die allgemeinen Anforderungen basierend auf der Anforderung OPS.2.3.A4 *Grundanforderungen an Verträge mit Anbietenden von Outsourcing* sowie weitere Aspekte der Informationssicherheit für Outsourcing-Vorhaben standardisieren. Das Test- und Freigabeverfahren für Outsourcing-Vorhaben SOLLTE in dieser Richtlinie geregelt sein. Darüber hinaus SOLLTEN Maßnahmen berücksichtigt sein, um Compliance-Risiken bei Anbietenden von Outsourcing sowie bei Sub-Dienstleistenden zu bewältigen.

### OPS.2.3.A10 Etablierung einer zuständigen Person für das Auslagerungsmanagement (S) [Personalabteilung]

Die verschiedenen Outsourcing-Vorhaben SOLLTEN durch eine zuständige Person für das Auslagerungsmanagement verwaltet werden. Die zuständige Person SOLLTE ernannt und die Befugnisse festgelegt und dokumentiert werden. Die zuständige Person SOLLTE als Schnittstelle in der Kommunikation zwischen den Nutzenden und Anbietenden von Outsourcing eingesetzt werden. Darüber hinaus SOLLTE die zuständige Person Berichte über das Outsourcing in regelmäßigen Abständen und anlassbezogen anfertigen und der Institutionsleitung übergeben. In der Vertragsgestaltung SOLLTE die zuständige Person einbezogen werden. Die zuständige Person SOLLTE ein angemessenes Kontingent von Arbeitstagen für die Aufgaben des Auslagerungsmanagements eingeräumt bekommen. Darüber hinaus SOLLTE die zuständige Person hinsichtlich Informationssicherheit geschult und sensibilisiert sein.

## OPS.2.3.A11 Führung eines Auslagerungsregisters (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE ein Auslagerungsregister erstellen und pflegen, dass die Dokumentation der Outsourcing-Prozesse und Vorhaben in der Institution zentralisiert. Dieses SOLLTE auf der Basis der Anforderungsprofile erstellt werden und Informationen zu den Anbietenden von Outsourcing, Leistungskennzahlen, Kritikalität des Prozesses, abgeschlossene Verträgen und Vereinbarungen sowie Änderungen enthalten. Änderungen am Auslagerungsregister SOLLTEN geeignet nachgehalten werden.

## OPS.2.3.A12 Erstellung von Auslagerungsberichten (S)

Die zuständige Person für das Auslagerungsmanagement SOLLTE regelmäßig interne Auslagerungsberichte auf Basis des Auslagerungsregisters erstellen. Diese Auslagerungsberichte SOLLTEN den aktuellen Status des Outsourcing-Vorhabens mit allgemeinen Problemen und Risiken sowie Aspekte der Informationssicherheit enthalten. Der Auslagerungsbericht SOLLTE der Institutionsleitung vorgelegt werden.

## OPS.2.3.A13 Bereitstellung der erforderlichen Kompetenzen bei der Vertragsgestaltung (S) [Institutionsleitung]

Die Verträge SOLLTEN durch verschiedene Vertreter aus unterschiedlichen Bereichen gestaltet werden. Dabei SOLLTE ein Interessenkonflikt zwischen operativem Geschäft und Informationssicherheit vermieden werden.

## OPS.2.3.A14 Erweiterte Anforderungen an Verträge mit Anbietenden von Outsourcing (S)

Mit Anbietenden von Outsourcing SOLLTE vereinbart werden, auf welche Bereiche und Dienste die Anbietenden im Netz der Nutzenden von Outsourcing zugreifen dürfen. Der Umgang mit anfallenden Metadaten SOLLTE geregelt werden. Die Nutzenden SOLLTEN Leistungskennzahlen für die Anbietenden von Outsourcing definieren und im Vertrag festlegen. Für den Fall, dass die vereinbarten Leistungskennzahlen unzureichend erfüllt werden, SOLLTEN mit den Anbietenden von Outsourcing Konsequenzen, wie z. B. Vertragsstrafen, festgelegt werden. Die Verträge SOLLTEN Kündigungsoptionen, um das Outsourcing-Verhältnisses aufzulösen, enthalten. Hierbei SOLLTE auch geregelt sein, wie das Eigentum der Nutzenden von Outsourcing zurückgegeben wird. Im Vertrag SOLLTEN Verantwortlichkeiten hinsichtlich des Notfall- und Krisenmanagements definiert und benannt werden.

## OPS.2.3.A15 Anbindung an die Netze der Outsourcing-Partner (S)

Bevor das Datennetz der Nutzenden an das Datennetz der Anbietenden von Outsourcing angebunden wird, SOLLTEN alle sicherheitsrelevanten Aspekte schriftlich vereinbart werden. Es SOLLTE geprüft und dokumentiert werden, dass die Vereinbarungen für die Netzanbindung eingehalten werden. Das geforderte Sicherheitsniveau SOLLTE nachweislich bei den Anbietenden von Outsourcing umgesetzt und überprüft werden, bevor die Netzanbindung zu den Nutzenden von Outsourcing aktiviert wird. Bevor die Netze angebunden werden, SOLLTE mit Testdaten die Verbindung getestet werden. Gibt es Sicherheitsprobleme auf einer der beiden Seiten, SOLLTE festgelegt sein, wer informiert und wie eskaliert wird.

## OPS.2.3.A16 Prüfung der Anbietenden von Outsourcing (S)

Die Anbietenden von Outsourcing SOLLTEN hinsichtlich der vertraglich festgelegten Sicherheitsanforderungen überprüft und die Resultate dokumentiert werden. Die Anbietenden von Outsourcing sind in regelmäßigen Abständen und anlassbezogen zu auditieren.

### OPS.2.3.A17 Regelungen für den Einsatz des Personals von Anbietenden von Outsourcing (S)

Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN schriftlich verpflichtet werden, einschlägige Gesetze, Vorschriften sowie die Regelungen der Nutzenden von Outsourcing einzuhalten. Die Beschäftigten der Anbietenden von Outsourcing SOLLTEN geregelt in ihre Aufgaben eingewiesen und über bestehende Regelungen zur Informationssicherheit unterrichtet werden. Für die Beschäftigten der Anbietenden von Outsourcing SOLLTEN Vertretungsregelungen existieren. Es SOLLTE ein geregeltes Verfahren festgelegt werden, das beschreibt, wie das Auftragsverhältnis mit den Beschäftigten der Anbietenden von Outsourcing beendet wird. Fremdpersonal der Anbietenden von Outsourcing, das kurzfristig oder nur einmal eingesetzt wird, SOLLTE wie Besuchende behandelt werden.

### OPS.2.3.A18 Überprüfung der Vereinbarungen mit Anbietenden von Outsourcing (S)

Vereinbarungen mit Anbietenden von Outsourcing hinsichtlich der Angemessenheit der festgelegten Sicherheitsanforderungen sowie sonstigen Sicherheitsanforderungen SOLLTEN in regelmäßigen Abständen und anlassbezogen überprüft werden. Vereinbarungen mit Anbietenden von Outsourcing mit unzureichend festgelegten Sicherheitsanforderungen SOLLTEN nachgebessert werden. Die Anbietenden von Outsourcing SOLLTEN dazu verpflichtet werden, bei veränderter Gefährdungs- oder Gesetzeslage, die festgelegten Sicherheitsanforderungen nachzubessern.

### OPS.2.3.A19 Überprüfung der Handlungsalternativen hinsichtlich einer geplanten oder ungeplanten Beendigung eines Outsourcing-Verhältnisses (S) [Beschaffungsstelle]

Handlungsalternativen SOLLTEN entwickelt werden für den Fall einer geplanten oder ungeplanten Beendigung des Outsourcing-Verhältnisses. Das Resultat SOLLTE in einem Maßnahmenkatalog für geplante und ungeplante Beendigung des Outsourcing-Verhältnisses dokumentiert werden. Dabei SOLLTEN auch alternative Anbietende von Outsourcing ermittelt werden, die über das notwendige Niveau an Informationssicherheit verfügen, um den Prozess sicher umzusetzen. Dies SOLLTE in regelmäßigen Abständen und anlassbezogen geprüft werden.

### OPS.2.3.A20 Etablierung sowie Einbeziehung von Anbietenden von Outsourcing im Notfallkonzept (S) [Notfallbeauftragte]

Ein Notfallkonzept SOLLTE in der Institution etabliert sein. Dies SOLLTE auf der Basis einer Business-Impact-Analyse basieren und die Abhängigkeiten der ausgelagerten Prozesse mit den intern verbliebenen Prozessen berücksichtigen. Das Notfallkonzept SOLLTE den Anbietenden von Outsourcing in seiner Notfallvorsorge und -bewältigung berücksichtigen und mit diesem abgestimmt sein. Dabei SOLLTEN die Schnittstellen zu Anbietenden von Outsourcing mit Verantwortlichen benannt und besetzt werden, um einen Informationsaustausch sowie eine effektive Kollaboration in einer Not- oder Krisensituation zu ermöglichen. Gemeinsame Not- und Krisenfallpläne SOLLTEN für eine Störung oder einen Ausfall der Anbietenden von Outsourcing erstellt werden. Standardisierte Protokolle und Berichte SOLLTEN zur Meldung von Sicherheitsvorfällen etabliert werden.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

### OPS.2.3.A21 Abschluss von ESCROW-Verträgen bei softwarenahen Dienstleistungen (H)

Wird Software von Anbietenden von Outsourcing bezogen, SOLLTE ein ESCROW-Vertrag abgeschlossen werden. Dieser SOLLTE Verwertungs- und Bearbeitungsrechte der Software sowie Herausgabefälle des Quellcodes regeln. Darüber hinaus SOLLTE festgelegt werden, wie häufig der Quellcode hinterlegt und dokumentiert wird. Weiterhin SOLLTEN Geheimhaltungspflichten über den hinterlegten Quellcode und die zugehörige Dokumentation geregelt werden.

### OPS.2.3.A22 Durchführung von gemeinsamen Notfall- und Krisenübungen (H) [Notfallbeauftragte]

Gemeinsame Notfall- und Krisenübungen mit den Anbietenden von Outsourcing SOLLTEN durchgeführt und dokumentiert werden (siehe DER.4 *Notfallmanagement*). Das Resultat der Übung SOLLTE dazu genutzt werden, um das Notfallkonzept sowie insbesondere die gemeinsamen Maßnahmenpläne zu verbessern. Die Notfall- und Krisenübungen SOLLTEN regelmäßig und anlassbezogen durchgeführt werden.

### OPS.2.3.A23 Einsatz von Verschlüsselungen (H)

Sensible Daten SOLLTEN angemessen verschlüsselt werden, wenn sie zum Anbietenden von Outsourcing übertragen werden. Die abgelegten Daten SOLLTEN durch eine Datenverschlüsselung oder eine Verschlüsselung des Speichermediums geschützt werden. Nach Möglichkeit SOLLTE eine vom BSI geprüfte und freigegebene Verschlüsselungssoftware genutzt werden.

### OPS.2.3.A24 Sicherheits- und Eignungsüberprüfung von Mitarbeitenden (H) [Personalabteilung]

Mit externen Anbietenden von Outsourcing SOLLTE vertraglich vereinbart werden, dass die Vertrauenswürdigkeit des eingesetzten Personals geeignet überprüft wird. Dazu SOLLTEN gemeinsam Kriterien festgelegt und dokumentiert werden.

### OPS.2.3.A25 Errichtung und Nutzung einer Sandbox für eingehende Daten vom Anbietenden von Outsourcing (H)

Für eingehende Daten vom Anbietenden von Outsourcing SOLLTE eine Sandbox eingerichtet werden. Hierbei SOLLTEN E-Mail-Anhänge in der Sandbox standardisiert geöffnet werden. Updates und Anwendungen eines softwarenahen Anbietenden von Outsourcing SOLLTEN in der Sandbox initial getestet werden.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel A.15.2 "Steuerung der Dienstleistungserbringung von Lieferanten" Vorgaben für die Steuerung von Anbietenden von Outsourcing. In der DIN ISO 37500:2015-08 werden im "Leitfaden Outsourcing" weiterführende Informationen zum Umgang mit Anbietenden von Outsourcing aufgeführt.

Des Weiteren wird in der ISO 27002:2021 das Outsourcing-Verhältnis von Kapitel 5.19 bis 5.22 detailliert aufgeführt und spezifiziert somit die Vorgaben der ISO/IEC 27001:2013.

Das Information Security Forum (ISF) definiert in seinem Standard "The Standard of Good Practice for Information Security" verschiedene Anforderungen (SC1) an Anbietende von Outsourcing.

Der "Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland" des Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Bitkom) liefert Informationen, wie Geschäftsprozesse an Anbietenden von Outsourcing ausgelagert werden können.

Ebenso hat die Bitkom den "Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis" herausgegeben, die rechtlichen Aspekte von Outsourcing behandelt.

Das National Institute of Standards and Technology (NIST) nennt in der NIST Special Publication 800-53 Anforderungen an Anbietenden von Outsourcing.