Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein ORP.5 Compliance Management (Anforderungsmanagement)

1. Einleitung

In jeder Institution gibt es aus den verschiedensten Richtungen gesetzliche, vertragliche und sonstige Vorgaben wie z.B. interne Richtlinien, die beachtet werden müssen. Viele davon haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement. Die Anforderungen sind je nach Branche, Land und anderen Rahmenbedingungen unterschiedlich. Weiterhin unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen durch angemessene Überwachungsmaßnahmen (neudeutsch: Compliance) sicherstellen und ein Compliance Management System betreiben.

Ziel des Compliance Managements ist es, jederzeit den Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche der Institution zu haben und geeignete Maßnahmen zu identifizieren und umzusetzen, um Verstöße gegen diese Anforderungen zu vermeiden.

Diese Aufgabe wird typischerweise an einen Mitarbeiter übertragen. Die Rolle wird im Folgenden mit „Compliance Manager“ bezeichnet. In einigen Institutionen wird z. B. auch die Bezeichnung „Anforderungsmanager“ benutzt. Sofern dies nicht durch andere Regelungen vorgeschrieben ist, müssen hierfür aber keine neuen Stellen geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justiziariat mit übernommen werden.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen, z. B. Sicherheitsmanagement, Datenschutzmanagement, Compliance Management, Controlling. Diese sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins ORP.5 *Compliance Management (Anforderungsmanagement)* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein ORP.5 Compliance Management (Anforderungsmanagement)

ORP.5.M1 Identifikation der Rahmenbedingungen (B)

Bei der Verarbeitung von Informationen sind eine Vielzahl von gesetzlichen oder vertraglichen Rahmenbedingungen zu beachten. Diese variieren sehr stark in Abhängigkeit von der Art der Institution, der Branche und den Geschäftsprozessen.

Typische Bereiche der Informationsverarbeitung, die besonderen gesetzlichen Regelungen unterliegen, sind:

- Schutz personenbezogener Daten,
- Einsatz von kryptographischen Verfahren,
- Schutz von geistigem Eigentum,
- ordnungsgemäßer Betrieb von IT-Systemen, inklusive Überwachung, Protokollierung und Auswertung,
- Langzeitspeicherung von Daten.

Abhängig von dem Land, in dem die Informationen verarbeitet werden und ihrem speziellen Einsatzzweck können noch eine Vielzahl von weiteren rechtlichen Regelungen existieren. Diese einzeln zu nennen, würde den Rahmen dieses Dokumentes sprengen. In diversen Bereichen des IT-Grundschutzes werden länder- oder branchenspezifische Gesetze angesprochen, wie z. B. zu Kryptographie, Outsourcing oder Archivierung. Dies sind aufgrund der Vielzahl möglicher gesetzlicher Rahmenbedingungen jeweils nur Beispiele ohne Anspruch auf Vollständigkeit oder Aktualität.

Übersicht über rechtliche Rahmenbedingungen

Alle für die Geschäftsprozesse und Informationsverarbeitung, den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden. Es ist dabei zu beachten, dass gesetzliche Vorschriften sich häufig ebenfalls auf Landes- und Regionalebene unterscheiden. Als Konsequenz müssen unter Umständen für jede Lokation jeweils die dort gültigen Gesetze eingehalten werden. Ebenso ist zu berücksichtigen, dass je nach Art der Geschäftsprozesse und dem Einsatzzweck der IT-Systeme (z. B. Büroumgebung, Prozesssteuerung) verschiedene Vorschriften gelten können.

Insbesondere müssen

- alle angewandten betrieblichen Praktiken und Vorgehensweisen,
- alle im Rahmen der geschäftlichen Tätigkeiten verarbeiteten Informationen,
- alle installierten IT-Systeme (Hardware- und Software) sowie
- die zum Betrieb der Geschäftsprozesse und IT-Systeme notwendige physikalische Infrastruktur

die gültigen gesetzlichen Vorschriften erfüllen. Alle Änderungen gesetzlicher Auflagen müssen erfasst und die für die Institution relevante Änderungen berücksichtigt werden.

Typischerweise gibt es in den verschiedenen Bereichen einer Institution Übersichten über die Anforderungen, die in diesen Bereichen und für deren Geschäftsprozesse relevant sind. Nicht immer sind dies formalisierte Übersichten, sondern oftmals Einzelinformationen in verschiedenen Strukturen und Wissen in den Köpfen von Experten. Durch die Komplexität vieler Geschäftsprozesse und

Organisationsstrukturen sowie durch eine zunehmende Vielfalt an Vorgaben aus der internationalen Zusammenarbeit können sich hierbei schnell eine große Anzahl verschiedener Anforderungen ergeben. Deswegen sollte das vorhandene Wissen über die verschiedenen gesetzlichen, vertraglichen und sonstigen Vorgaben zentral zusammengetragen und, wenn nötig, ergänzt werden.

ORP.5.M2 Beachtung der Rahmenbedingungen (B)

Führungskräfte, welche die rechtliche Verantwortung für die Institution vor Ort tragen, müssen für die Identifizierung und Dokumentation der anzuwendenden gesetzlichen Vorschriften sorgen. Idealerweise sollte ein Jurist oder Rechtsexperte beauftragt werden. Falls innerhalb der Institution das erforderliche Wissen oder die nötigen Ressourcen nicht zur Verfügung stehen, sollte externe Rechtsberatung eingeholt werden. Da nicht alle Mitarbeiter sämtliche Gesetze und Regelungen kennen müssen, sollten dabei die für die einzelnen Bereiche der Institution relevanten gesetzlichen und vertraglichen Vorgaben herausgearbeitet werden. Um deren Einhaltung zu überwachen, können in den einzelnen Bereichen Verantwortliche benannt werden. So ist der betriebliche Datenschutzbeauftragte dafür verantwortlich, auf die Einhaltung der gültigen Datenschutzvorschriften sowie für die Erstellung und Einhaltung eines institutionsweit gültigen Regelwerks zum Schutz personenbezogener Daten hinzuwirken. Die IT-Leitung muss dagegen z. B. für die Definition und Dokumentation des Lizenzmanagements sorgen.

Natürlich ist auch jeder einzelne Mitarbeiter und insbesondere das Führungspersonal für die Umsetzung der Regelungen zu rechtlichen Aspekten und für die Überwachung der Einhaltung in seinem Arbeitsumfeld verantwortlich (siehe ORP.5.M3 *Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen*).

ORP.5.M3 ENTFALLEN (B)

Die zugehörige Anforderung ist entfallen.

ORP.5.M4 Konzeption und Organisation des Compliance Managements (S)

Typischerweise ergeben sich aus den verschiedenen Tätigkeiten einer Institution eine Vielzahl verschiedener gesetzlicher, vertraglicher und anderer rechtlicher Vorgaben. Die Identifikation dieser Anforderungen und der Umgang mit diesen kann schnell sehr komplex werden. Dafür sollten Verantwortliche benannt und deren Aufgaben im Bereich Compliance Management festgelegt werden. Die entsprechende Rolle wird häufig als "Compliance Manager" bezeichnet. Je nach Art und Größe der Institution kann es sinnvoll sein, einen oder mehrere Compliance Manager zu benennen.

In einigen Institutionen wird auch die Bezeichnung "Anforderungsmanager" benutzt. Sofern dies nicht durch andere Regelungen vorgeschrieben ist, muss hierfür aber keine neue Stelle geschaffen werden. Die Aufgabe kann beispielsweise vom Sicherheitsmanagement, der Revision, dem Controlling oder dem Justiziariat mit übernommen werden.

Die Benennung eines zentralen Compliance Manager hat den Vorteil, dass dieser einen Überblick über die gesamte Institution hat, wodurch Doppelarbeiten und Konflikte frühzeitig erkannt und vermieden werden können. Mehrere Compliance Manager in den verschiedenen Bereichen einer Institution können andererseits meist besser die Bedürfnisse der von ihnen betreuten Zielgruppe abdecken. Im Folgenden wird der besseren Lesbarkeit wegen immer im Singular auf die Rolle des Compliance Managers Bezug genommen.

Zu den Aufgaben eines Compliance Managers (für die von ihm betreuten Bereiche) gehören:

- Alle für die wesentlichen Geschäftsprozesse und Informationen sowie für den Betrieb von IT-Systemen und der zugehörigen physischen Infrastruktur zu beachtenden gesetzlichen, vertraglichen und sonstigen Vorgaben müssen identifiziert und dokumentiert werden (siehe ORP.5.M1 *Identifikation der rechtlichen Rahmenbedingungen*).
- Die Anforderungen sind strukturiert zu erfassen und aus den verschiedenen Bereichen zusammenzuführen und zu konsolidieren.
- Um die einzelnen identifizierten Anforderungen zu erfüllen und angemessene Maßnahmen umzusetzen, müssen Verantwortliche benannt werden. Der Compliance Manager sollte regelmäßig überprüfen, ob die ergriffenen Maßnahmen geeignet sind, um die Anforderungen abzudecken.

- Häufig müssen Anforderungen auch zunächst interpretiert und auf die Gegebenheiten der jeweiligen Institution übersetzt werden, da die meisten Gesetze und Vorgaben eher Ziele und Erwartungen formulieren, nicht aber wie deren Umsetzung konkret auszugestalten ist.
- Alle Arten der genannten Anforderungen gehen auch jeweils auf eine bestimmte Zielgruppe zurück, die deren Einhaltung fordert oder prüft. Bei der Identifikation der Anforderungen sollte auch immer die Zielgruppe dokumentiert werden, um deren Bedürfnisse zu erfüllen. Dies erspart später viele Anpassungsarbeiten. Bei gesetzlichen Anforderungen ist es z. B. sinnvoll, festzuhalten, welche Instanz (also z. B. welche Aufsichtsstelle) deren Einhaltung prüft und in welcher Form hierfür die Informationen aufbereitet werden müssen.

In der folgenden Tabelle finden sich hierzu einige Beispiele:

Anforderungen	**Zielgruppe**	**Verantwortlicher Compliance Manager**
Datenschutz-Gesetze	Datenschutz-Aufsicht	Behördlicher oder betrieblicher Datenschutzbeauftragter
Arbeitsrecht	Personalvertretung	Personalreferat
Strafrecht	Strafverfolgungsbehörden	Justiziariat / Hausjurist
Verträge	Dienstleister / Kunden	Einkauf / Vertrieb
Sonstige Anforderungen	Kooperationspartner	Fachabteilung

Tabelle 1: Zuordnung von Anforderungen zu Zielgruppen und Compliance Manager

Zusammenarbeit mit Sicherheitsmanagement

Die Informationssicherheit ist direkt oder indirekt ein zu beachtender Aspekt in fast allen Anforderungsbereichen. Dabei ist der Informationssicherheitsbeauftragte nur in wenigen Fällen der Compliance Manager. Compliance Manager und Informationssicherheitsbeauftragter müssen daher regelmäßig zusammenarbeiten, um einerseits die Sicherheitsanforderungen aus den verschiedenen Bereichen ins Compliance Management zu integrieren und andererseits die als sicherheitsrelevant identifizierten Anforderungen in Sicherheitsmaßnahmen zu überführen und deren Umsetzung zu kontrollieren.

Sicherheitsanforderungen ergeben sich in erster Linie durch die Auslegung allgemeiner Rechtsvorschriften, teilweise aus Spezialgesetzen sowie aus tätigkeits- oder branchenbezogenen Vorschriften, die die Sicherheit bestimmter Systeme, Dienstleistungen oder Tätigkeiten regeln. Dazu kommen zivilrechtliche Pflichten, deren (schuldhafte) Verletzung zu Haftung des Verantwortlichen führen kann. Beispiele sind

- Datenschutzgesetze
- KWG, KonTraG, MaRisk der BaFin
- Urheberrechtsgesetz
- TKG, TMG
- ITSiG
- Verträge, Allgemeine Geschäftsbedingungen, etc.
- Lizenzmanagement

Die als sicherheitsrelevant identifizierten Anforderungen sollten bei der Planung und Konzeption von Geschäftsprozessen, Anwendungen und IT-Systemen oder bei der Beschaffung neuer Komponenten einfließen.

ORP.5.M5 Ausnahmegenehmigungen (S)

In Einzelfällen kann es sinnvoll und notwendig sein, Ausnahmen von den in einer Sicherheitsrichtlinie getroffenen Regelungen zuzulassen. Ausnahmen sollten zwar möglichst vermieden werden, es ist aber auf jeden Fall besser, eine Ausnahme zuzulassen, als unnachgiebig auf Vorgaben zu bestehen, die im konkreten Einzelfall nicht einzuhalten sind. Sollten sich Ausnahmen häufen, ist dies ein Zeichen dafür, dass die vorhandenen Sicherheitsvorgaben überdacht und eventuell angepasst werden müssen.

Ausnahmen müssen aber in jedem Fall durch eine autorisierte Stelle genehmigt werden. Bei dem Genehmigungsverfahren sind sowohl Fachverantwortliche als die "Eigentümer" von Informationen und Anwendungen, als auch das Sicherheitsmanagement zu beteiligen. Für alle Ausnahmefälle muss gründlich überprüft werden, ob diese essentielle Sicherheitsvorgaben nicht untergraben. Dafür ist eine Risikobewertung vorzunehmen. Ausnahmen dürfen nur genehmigt werden, wenn dass ermittelte Risiko als tragbar eingestuft wurde.

Ausnahmegenehmigungen sollten zeitlich klar befristet werden. Es muss regelmäßig überprüft werden (spätestens alle 12 Monate), ob die Ausnahmegenehmigungen noch erforderlich sind und ob zeitlich befristete Ausnahmegenehmigungen wieder aufgehoben oder nach Ablauf verlängert wurden.

Anschließend muss eine schriftliche Begründung verfasst werden, die von den Verantwortlichen zu unterzeichnen ist.

Für die Erteilung von Ausnahmegenehmigungen sollte ein dokumentiertes Verfahren existieren. Es sollte mindestens folgendes dokumentiert werden:

- Begründung, warum eine Abweichung von den Sicherheitsvorgaben erforderlich ist und welche Regelung betroffen ist,
- Beschreibung der Ausgestaltung der Ausnahmegenehmigungen sowie Darstellung der Auswirkungen und Abgrenzung des betroffenen Bereichs, inklusive der Risikobewertung,
- Zeitpunkt der Einrichtung,
- Antragsteller und Genehmigender sowie
- Zeitraum der Befristungen.

Über genehmigte Abweichungen von den geltenden Sicherheitsvorgaben sind alle betroffenen Mitarbeiter zu informieren.

ORP.5.M6 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

ORP.5.M7 ENTFALLEN (S)

Die zugehörige Anforderung ist entfallen.

ORP.5.M8 Regelmäßige Überprüfungen des Compliance Managements (S)

Ebenso wie die Prozesse des Sicherheitsmanagements sollte auch das Compliance Management und die sich aus diesem ergebenden Anforderungen und Maßnahmen regelmäßig auf Effizienz und Effektivität überprüft werden (siehe auch DER.1.3 Audits und Revisionen). Es sollte regelmäßig geprüft werden, ob die Organisationsstruktur und die Prozesse des Compliance Managements noch angemessen sind.

In diesem Rahmen sollte auch überprüft werden, ob die in den verschiedenen Bereichen der Institution vorhandenen Geschäftsprozesse einerseits den rechtlichen Vorgaben und andererseits den Sicherheitsanforderungen genügen.

ORP.5.M9 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

ORP.5.M10 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

ORP.5.M11 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

Für den Umsetzungshinweis ORP.5 *Compliance Management (Anforderungsmanagement)* sind keine Quellenverweise vorhanden.