Bundesamt
für Sicherheit in der
Informationstechnik

ORP.5 Compliance Management (Anforderungsmanagement)

1. Beschreibung

1.1. Einleitung

In jeder Institution gibt es relevante gesetzliche, vertragliche und sonstige Vorgaben, wie z. B. interne Richtlinien, die beachtet werden müssen. Viele dieser Vorgaben haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement.

Die Anforderungen unterscheiden sich dabei je nach Branche, Land und anderen Rahmenbedingungen. Darüber hinaus unterliegt beispielsweise eine Behörde anderen externen Regelungen als eine Aktiengesellschaft. Die Leitungsebene der Institution muss die Einhaltung der Anforderungen („Compliance“) durch angemessene Überwachungsmaßnahmen sicherstellen.

Je nach Größe einer Institution kann diese verschiedene Managementprozesse haben, die sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen. Dazu zählen beispielsweise Informationssicherheitsmanagement, Datenschutzmanagement, Compliance Management und Controlling. Die verschiedenen Einheiten sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

1.2. Zielsetzung

Ziel des Bausteins ist es, aufzuzeigen, wie sich Zuständige einen Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche einer Institution verschaffen können. Dazu sind geeignete Sicherheitsanforderungen zu identifizieren und umzusetzen, um Verstöße gegen diese Vorgaben zu vermeiden.

1.3. Abgrenzung und Modellierung

Der Baustein ORP.5 *Compliance Management (Anforderungsmanagement)* ist für den gesamten Informationsverbund einmal anzuwenden.

Die Verpflichtung der Mitarbeitenden zur Einhaltung der in diesem Baustein identifizierten gesetzlichen, vertraglichen und sonstigen Vorgaben ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.2 *Personal* behandelt.

In diesem Baustein wird nicht auf spezifische Gesetze, vertragliche Regelungen oder sonstige Richtlinien eingegangen.

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 ORP.5 *Compliance Management (Anforderungsmanagement)* von besonderer Bedeutung.

2.1. Verstoß gegen rechtliche Vorgaben

Wird Informationssicherheit fehlerhaft oder nur spärlich umgesetzt, können Institutionen gegen gesetzliche Regelungen oder vertragliche Vereinbarungen verstoßen. Institutionen müssen außerdem viele verschiedene branchenspezifische, nationale und internationale rechtliche Rahmenbedingungen beachten. Da dies sehr komplex sein kann, können Anwendende unabsichtlich gegen rechtliche Vorgaben verstoßen oder dies sogar vorsätzlich in Kauf nehmen. So bieten z. B. viele Cloud-Dienstleistende ihre Services in einem internationalen Umfeld an. Damit unterliegen die Anbietenden oft anderen nationalen Gesetzgebungen. Häufig sehen Cloud-Anwendende nur auf niedrige Kosten und schätzen die zu beachtenden rechtlichen Rahmenbedingungen, wie Datenschutz, Informationspflichten, Insolvenzrecht, Haftung oder den Informationszugriff durch Dritte, falsch ein.

2.2. Unzulässige Weitergabe von Informationen

Durch falsches Verhalten von Mitarbeitenden kann es dazu kommen, dass schützenswerte Informationen unzulässig weitergegeben werden. So können beispielsweise vertrauliche Informationen in Hörweite fremder Personen diskutiert werden, etwa in Pausengesprächen von Konferenzen oder über Mobiltelefonate in öffentlichen Umgebungen. Ebenso denkbar ist, dass der oder die Vorgesetzte einer Fachabteilung Mitarbeitende verdächtigt, mit der Konkurrenz zusammenzuarbeiten. Um ihm dies nachzuweisen, bittet er oder sie den IT-Betrieb, „auf dem kleinen Dienstweg“ einen Einblick in die E-Mails dieser Mitarbeitenden zu erhalten. Der IT-Betrieb kommt der Bitte nach, ohne die hierfür notwendigen Zustimmungen einzuholen.

2.3. Unzureichende Identifikationsprüfung von Kommunikationspartnern und -partnerinnen

In persönlichen Gesprächen, am Telefon oder auch in E-Mails sind viele Mitarbeitende bereit, weit mehr Informationen preiszugeben, als sie das in z. B. in einem Brief oder in größerer Runde tun würden. Darüber hinaus wird die Identität der Kommunikationspartner und -partnerinnen in der Regel nicht hinterfragt, da dies als unhöflich empfunden wird. Ebenso werden häufig Berechtigungen nicht ausreichend geprüft, sondern aus der (behaupteten) Rolle implizit abgeleitet. So können Mitarbeitende eine E-Mail von angeblichen Bekannten ihrer Vorgesetzten erhalten, mit der vermeintlich die schnelle Überweisung eines ausstehenden Betrages vereinbart wurde. Oder eine fremde Person in Arbeitskleidung mit Montagekoffer erhält Zutritt zum Rechenzentrum, nachdem er etwas von "Wasserrohren" erwähnt.

2.4. Unbeabsichtigte Weitergabe interner Informationen

Bei der Weitergabe von Informationen kommt es immer wieder vor, dass neben den gewünschten Inhalten versehentlich auch andere Angaben übermittelt werden. Dadurch können vertrauliche Informationen in die falschen Hände geraten. Dabei kann es sich z. B. um alte Dateien oder Restinformationen auf weitergegebenen Datenträgern handeln. Auch könnten Benutzende falsche Daten übermitteln oder sie an falsche Empfänger versenden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins ORP.5 *Compliance Management (Anforderungsmanagement)* 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	Compliance-Beauftragte
Weitere Zuständigkeiten	Zentrale Verwaltung, Vorgesetzte, Institutionsleitung

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.

ORP.5.A1 Identifikation der Rahmenbedingungen (B) [Zentrale Verwaltung, Institutionsleitung]

Alle gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement MÜSSEN identifiziert und dokumentiert werden. Die für die einzelnen Bereiche der Institution relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben SOLLTEN in einer strukturierten Übersicht herausgearbeitet werden. Die Dokumentation MUSS auf dem aktuellen Stand gehalten werden.

ORP.5.A2 Beachtung der Rahmenbedingungen (B) [Vorgesetzte, Zentrale Verwaltung, Institutionsleitung]

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

Führungskräfte, die eine rechtliche Verantwortung für die Institution tragen, MÜSSEN für die Einhaltung der gesetzlichen, vertraglichen und sonstigen Vorgaben sorgen. Die Verantwortlichkeiten und Zuständigkeiten für die Einhaltung dieser Vorgaben MÜSSEN festgelegt sein.

Es MÜSSEN geeignete Maßnahmen identifiziert und umgesetzt werden, um Verstöße gegen relevante Anforderungen zu vermeiden. Wenn solche Verstöße erkannt werden, MÜSSEN sachgerechte Korrekturmaßnahmen ergriffen werden, um die Abweichungen zu beheben.

ORP.5.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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.

ORP.5.A4 Konzeption und Organisation des Compliance Managements (S) [Institutionsleitung]

In der Institution SOLLTE ein Prozess aufgebaut werden, um alle relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben mit Auswirkungen auf das Informationssicherheitsmanagement zu identifizieren. Es SOLLTEN geeignete Prozesse und Organisationsstrukturen aufgebaut werden, um basierend auf der Identifikation und Beachtung der rechtlichen Rahmenbedingungen, den Überblick über die verschiedenen rechtlichen Anforderungen an die einzelnen Bereiche der Institution zu gewährleisten. Dafür SOLLTEN Zuständige für das Compliance Management festgelegt werden.

Compliance-Beauftragte und Informationssicherheitsbeauftragte SOLLTEN sich regelmäßig austauschen. Sie SOLLTEN gemeinsam Sicherheitsanforderungen ins Compliance Management integrieren, sicherheitsrelevante Anforderungen in Sicherheitsmaßnahmen überführen und deren Umsetzung kontrollieren.

ORP.5.A5 Ausnahmegenehmigungen (S) [Vorgesetzte]

Ist es in Einzelfällen erforderlich, von getroffenen Regelungen abzuweichen, SOLLTE die Ausnahme begründet und durch eine autorisierte Stelle nach einer Risikoabschätzung genehmigt werden. Es SOLLTE ein Genehmigungsverfahren für Ausnahmegenehmigungen geben. Es SOLLTE eine Übersicht über alle erteilten Ausnahmegenehmigungen erstellt und gepflegt werden. Ein entsprechendes Verfahren für die Dokumentation und ein Überprüfungsprozess SOLLTE etabliert werden. Alle Ausnahmegenehmigungen SOLLTEN befristet sein.

ORP.5.A6 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.5.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements (S)

Es SOLLTE ein Verfahren etabliert sein, wie das Compliance Management und die sich daraus ergebenden Anforderungen und Maßnahmen regelmäßig auf ihre Effizienz und Effektivität überprüft werden (siehe auch DER.3.1 *Audits und Revisionen*). Es SOLLTE regelmäßig geprüft werden, ob die Organisationsstruktur und die Prozesse des Compliance Managements angemessen sind.

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.

ORP.5.A9 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.5.A10 ENTFALLEN (H)

Diese Anforderung ist entfallen.

ORP.5.A11 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO 19600:2014 „Compliance management systems - Guidelines“ Richtlinien für ein Compliance Management System.

Ebenso geht die ISO in der Norm ISO/IEC 27001:2013 „Information technology - Security technique - Code of practice for information security controls“ im Kapitel 18 auf Anforderungsmanagement ein.

Das Institut der Wirtschaftsprüfer (IDW) definiert in der IDW Verlautbarung IDW PS 980 „Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen“ Anhaltspunkte für die Prüfung von Compliance Management Systemen.