# **Compliance-Report: [Monat/Jahr]**

## **1. Einleitung**

**Zweck des Berichts:**

Dieser Compliance-Report dokumentiert den aktuellen Status der Einhaltung von regulatorischen und branchenspezifischen Anforderungen im Bereich IT-Sicherheit. Er dient dazu, Lücken aufzuzeigen und Handlungsempfehlungen zu geben, um die Compliance-Anforderungen nachhaltig zu erfüllen.

**Regulatorische Grundlagen:**

• ISO/IEC 27001 (Informationssicherheits-Managementsystem)

• NIS2-Richtlinie (Netz- und Informationssystemsicherheit)

• DORA (Digital Operational Resilience Act)

• DSGVO (Datenschutz-Grundverordnung)

• CRA (Cyber Resilience Act)

## **2. Compliance-Übersicht**

|  |  |  |
| --- | --- | --- |
| **Anforderung** | **Status** | **Bemerkungen** |
| ISO/IEC 27001 | Erfüllt | ISMS ist implementiert, jährliches Audit erfolgreich abgeschlossen. |
| NIS2 | Teilweise erfüllt | Schwachstellen-Management muss verbessert werden. |
| DORA | In Bearbeitung | Incident Response Framework in Implementierungsphase. |
| DSGVO | Erfüllt | Alle personenbezogenen Daten sind dokumentiert und geschützt. |
| CRA | Teilweise erfüllt | Teilweise erfüllt Schwachstellenanalyse wird regelmäßig durchgeführt, vollständige Dokumentation ausstehend. |

## **3. Detaillierte Compliance-Bewertung**

**3.1 ISO/IEC 27001**

**Status:** Erfüllt

**Details:**

• Das ISMS (Information Security Management System) wurde erfolgreich implementiert.

• Regelmäßige interne Audits und Risikoanalysen durchgeführt.

• Sicherheitsrichtlinien für Zugriffsmanagement und Datenverschlüsselung sind etabliert.

**Empfehlung:**

• Kontinuierliche Verbesserung der Sicherheitsmaßnahmen durch Lessons Learned aus Sicherheitsvorfällen.

• Schulungen zur Sensibilisierung aller Mitarbeiter für Sicherheitsrichtlinien.

**3.2 NIS2**

**Status:** Teilweise erfüllt

**Details:**

• Anforderungen an die Netzwerk- und Informationssicherheit werden größtenteils erfüllt.

• Defizite bestehen im Bereich des Schwachstellenmanagements und der Meldung von Vorfällen.

**Empfehlung:**

• Implementierung eines automatisierten Schwachstellen-Managementsystems.

• Einführung eines zentralisierten Vorfallmeldesystems.

**3.3 DORA**

**Status:** In Bearbeitung

**Details:**

• Aufbau eines Incident Response Frameworks begonnen, jedoch noch nicht abgeschlossen.

• Teilweise Umsetzung eines SOCs zur Überwachung und Behebung von Vorfällen.

**Empfehlung:**

• Vollständige Implementierung des Incident Response Frameworks bis [Zieldatum].

• Einführung eines regelmäßigen SOC-Reportings zur Überwachung der Resilienz.

**3.4 DSGVO**

**Status:** Erfüllt

**Details:**

• Alle personenbezogenen Daten sind dokumentiert, klassifiziert und durch Verschlüsselung geschützt.

• Datenschutzrichtlinien wurden von allen Mitarbeitern unterzeichnet und eingehalten.

• Datenverarbeitungsverträge (DPA) mit allen relevanten Dienstleistern abgeschlossen.

**Empfehlung:**

• Regelmäßige Überprüfung der Datenschutzprozesse, um neue Anforderungen frühzeitig zu berücksichtigen.

• Durchführung eines internen Audits im nächsten Quartal.

**3.5 CRA**

**Status:** Teilweise erfüllt

**Details:**

• Regelmäßige Schwachstellenanalysen werden durchgeführt.

• Fehlende vollständige Dokumentation der Sicherheitsprozesse.

**Empfehlung:**

• Erstellung einer vollständigen Sicherheitsdokumentation, die Schwachstellenmanagement, Asset-Management und Zugriffsmanagement abdeckt.

• Integration eines kontinuierlichen Sicherheitsbewertungsprozesses.

## **4. Festgestellte Lücken und Risiken**

|  |  |  |  |
| --- | --- | --- | --- |
| **Anforderung** | **Lücke** | **Risikobewertung** | **Empfehlung** |
| NIS2 | Unzureichendes Schwachstellenmanagement | Hoch | Automatisiertes Schwachstellenmanagementsystem. |
| DORA | Unvollständiges Incident Response Framework | Mittel | Abschluss der Framework-Implementierung. |
| CRA | Fehlende Sicherheitsdokumentation | Mittel | Erstellung der Dokumentation bis [Datum]. |

## **5. Maßnahmenplan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Maßnahme** | **Zuständig** | **Frist** | **Status** |
| Einführung eines Schwachstellenmanagements | IT-Sicherheitsabteilung | [Datum] | In Bearbeitung |
| Abschluss des Incident Response Frameworks | SOC-Team | [Datum] | Offen |
| Erstellung einer vollständigen Sicherheitsdokumentation | Compliance-Team | [Datum] | Offen |

## **6. KPIs zur Erfolgsmessung**

|  |  |  |
| --- | --- | --- |
| **KPI** | **Aktueller Wert** | **Zielwert** |
| Mean Time to Detect (MTTD) | [X Minuten/Stunden] | 10% Verbesserung |
| Anzahl geschlossener Schwachstellen | [X] | Vollständige Abdeckung |
| Incident Response Prozesse vollständig | [50%] | 100% bis [Datum] |

## **7. Lessons Learned**

• **Erfolgreiche Maßnahmen:** DSGVO-Prozesse sind vollständig umgesetzt und bieten eine gute Basis für weitere Compliance-Bestrebungen.

• **Verbesserungspotenziale:** Verzögerungen bei der Umsetzung von DORA zeigen die Notwendigkeit besserer Projektplanung und Ressourcenverteilung.

## **8. Fazit und nächste Schritte**

**Zusammenfassung:**

Das Unternehmen hat Fortschritte bei der Einhaltung der Compliance-Anforderungen gemacht, insbesondere in den Bereichen ISO 27001 und DSGVO. Allerdings bestehen weiterhin Lücken in der Umsetzung von NIS2, DORA und CRA, die zeitnah adressiert werden müssen.

**Empfohlene nächste Schritte:**

1. Beschleunigung der Implementierung des Incident Response Frameworks.

2. Einführung eines zentralisierten Schwachstellenmanagementsystems.

3. Erstellung und Pflege einer umfassenden Sicherheitsdokumentation.

**Bericht erstellt von:**

[Name des Compliance-Managers]

[Position]

[Datum]