DORA Compliance Blueprint: Ein Schritt-für-Schritt-Leitfaden zur Stärkung der digitalen operationellen Resilienz

Das Gesetz zur digitalen operationellen Resilienz (DORA) zielt darauf ab, die digitale Resilienz von Finanzinstituten innerhalb der Europäischen Union zu stärken. Um den Anforderungen von DORA gerecht zu werden, sollten Sie die folgenden Schritte in Betracht ziehen:

1. **Prüfen Sie die Anwendbarkeit:**
   - Bestimmen Sie, ob Ihr Unternehmen unter den Geltungsbereich von DORA fällt, der verschiedene Finanzinstitute und kritische Drittanbieter umfasst.
2. **Etablieren Sie ein IKT-Risikomanagement-Framework:**
   - Entwickeln Sie ein umfassendes Framework zur Identifizierung, Bewertung und Verwaltung von Informations- und Kommunikationstechnologie (IKT)-Risiken.
   - Stellen Sie sicher, dass das Framework alle Phasen des IKT-Systemlebenszyklus
3. **Implementieren Sie Vorfallberichterstattungsverfahren:**
   - Richten Sie Prozesse ein, um schwerwiegende IKT-bezogene Vorfälle schnell zu erkennen, zu klassifizieren und den zuständigen Behörden zu melden.
   - Führen Sie Aufzeichnungen über Vorfälle und Reaktionen zur Sicherstellung der Verantwortlichkeit.
4. **Führen Sie Tests der digitalen operationellen Resilienz durch:**
   - Testen Sie regelmäßig IKT-Systeme, um die Resilienz gegenüber Störungen zu bewerten.
   - Integrieren Sie Bedrohungs-getriebenes Penetrationstesting (TLPT), um Cyberangriffe zu simulieren und die Abwehrmechanismen zu evaluieren.
5. **Verwalten Sie Risiken von Drittanbietern im Bereich IKT:**
   - Bewerten und überwachen Sie die Risiken im Zusammenhang mit Drittanbieter-IKT-Dienstleistern.
   - Stellen Sie sicher, dass vertragliche Vereinbarungen Bestimmungen für Risikomanagement und die Einhaltung von DORA enthalten.
6. **Fördern Sie den Informationsaustausch:**
   - Beteiligen Sie sich an Informationsaustausch-Vereinbarungen mit anderen Finanzinstituten, um Cyber-Bedrohungsinformationen und Best Practices auszutauschen
7. **Bereiten Sie sich auf die behördliche Aufsicht vor:**
   - Seien Sie auf die Aufsicht durch zuständige Behörden vorbereitet, einschließlich möglicher Audits und Bewertungen.
   - Führen Sie umfassende Dokumentationen über Ihre Compliance-Bemühungen und IKT-Risikomanagement-Aktivitäten.

Durch die Befolgung dieses Leitfadens können Organisationen ihre digitale operationelle Resilienz stärken und die Anforderungen von DORA erfüllen.