jamf

Compliance-Verwaltung

für Einsteiger

Was ist Compliance?

Compliance bedeutet einfach, dass etwas sich an Gesetze, Gesundheits- und Sicherheitsstandards, oder Daten- und Sicherheitsanforderungen hält.

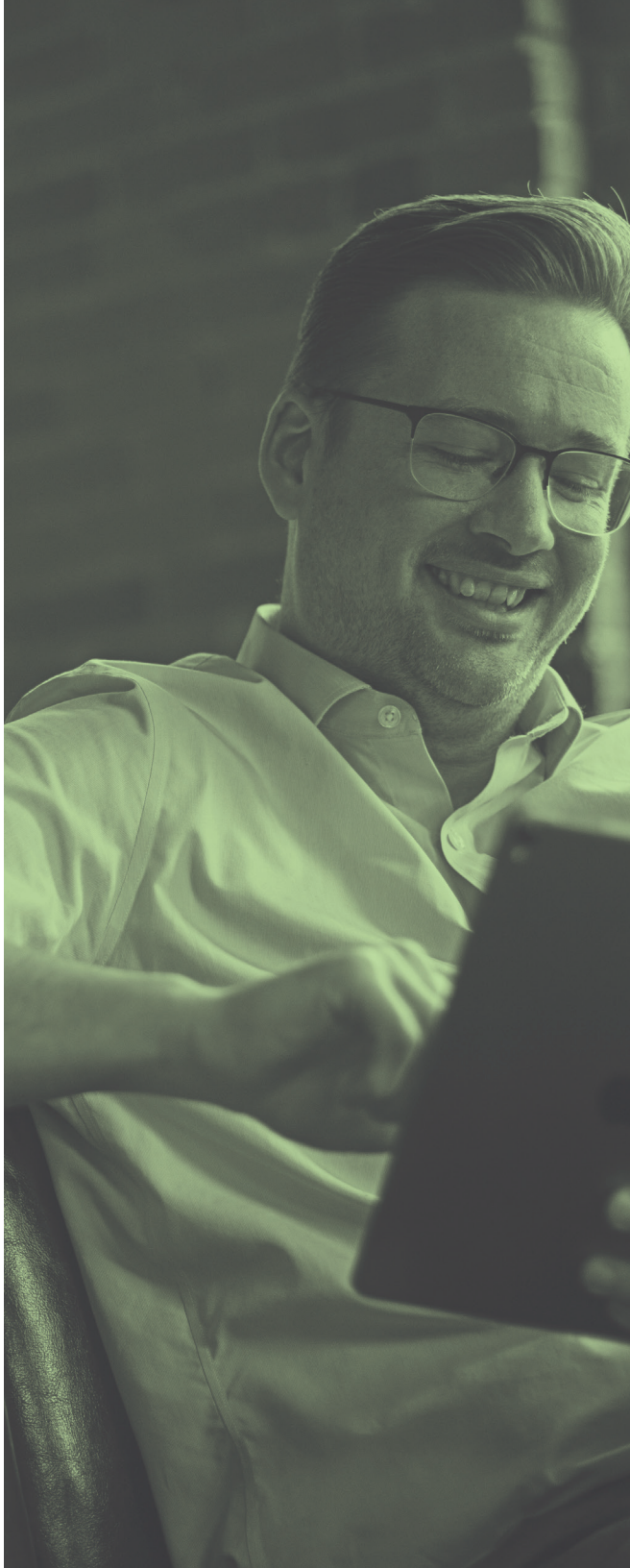
Klingt einfach, oder?

Aber warten Sie lieber.

Aufgrund der spezifischen Natur Ihrer Organisation kann Compliance für Sie etwas ganz anderes bedeuten als für die Schule am Ende der Straße oder das Krankenhaus an der andere Seite der Stadt. Deshalb sollte jede Organisation ihre eigenen Compliance-Standards entwerfen und Systeme aufbauen, die sicherstellen, dass ihre Mitarbeiter sich daran halten können.

Es gibt einige verschiedene Arten von Regulierung, die einen Compliance Plan erfordern:

- **Rechtsvorschriften**, wie Antidiskriminierung, Anti-Sklaverei und Bestimmungen gegen die Korruption
- **Branchenstandards**, wie Qualitätsnormen oder Datenschutzregeln
- **Sicherheit** wie den Schutz eines physischen Standorts, um die Kontrolle über Geräte zu gewährleisten und Daten geheim zu halten.
- **Von der Organisation bestimmte Regeln und Aufgaben** wie Umweltauswirkung oder Verhaltensanforderungen für Anbieter



Was ist Compliance?

Bei jedem dieser Compliance-Bereiche muss die Organisation den juristischen Auswirkungen, die Auswirkungen auf das Personal und die Auswirkungen auf Schüler, Patienten oder Kunden in Betracht ziehen.

Und jede Branche hat einen eigenen Satz von Rechtsvorschriften, Standards und Sicherheitsanforderungen, wie etwa folgende:

- **Organisationen im Gesundheitswesen** müssen in den USA dem Gesetz HIPAA folgen
- **Hochschul**einrichtungen müssen sich dort an FERPA halten
- **Finanzinstitutionen** müssen sich eng an die Regeln und Vorschriften der FDIC halten
- **Regierungsbehörden** müssen sich an FIPS (Federal Information Processing Standards) halten und sicherstellen, dass die drei Klassifizierungskategorien streng eingehalten werden.

Das sind viele Vorschriften, die man einhalten muss!
Aber das ist absolut wichtig.

Was kann passieren, wenn Unternehmen die Compliance ignorieren?

Wir müssen nicht raten, was passieren kann. Wir haben Beispiele dafür, die täglich und überall geschehen:

- Datenschutzverletzungen
- Datenlecks
- Finanzielle Verluste: Strafen oder Gebühren
- Verlust von Kunden, Accounts oder Stellen
- Rufschädigung

Hier sind nur drei Beispiele, die es international Schlagzeilen machten:

1. Ein globales Handelsunternehmen ließ es zu, dass die Kredit- und Debitkartendaten von 110 Millionen Kunden aufgrund in einer Schwachstelle bei einer App von Drittanbietern gestohlen wurden. Der Ruf des Unternehmens wurde schwer geschädigt, und es musste 18,5 Millionen US-Dollar Strafe zahlen.

2. Eine große und bekannte professionelle Networking-Website zahlte für Passwortlecks eine Strafgebühr von 1,25 Millionen US-Dollar und hatte dann kürzlich ein Datenleck, das über 700 Millionen Benutzer betraf und auf eine Schwachstelle in der API zurückzuführen war. Das hat ihren Ruf beeinträchtigt und wird wahrscheinlich auch Geld kosten.

3. Zwei große soziale Netzwerke, eines in China und eines in den USA, hatten Datenschutzverletzungen, die 538 bzw. 533 Millionen Benutzer betrafen und mehr als eine Milliarde E-Mail-Adressen und Telefonnummern enthüllten.

In allen diesen Fällen hätten korrekte Compliance-Verfahren diese Probleme vorher aufhalten können.

Was ist Compliance-Management?

Compliance-Management bezeigt sich darauf, wie gut Sie die Compliance verwalten.

Es sind die Richtlinien und Verfahren ihrer Organisation, um die Compliance in allen Bereichen zu gewährleisten. Das sind die digitalen Tools, die Sie verwenden, um Compliance zu gewährleisten. Und vor allem betrifft das die Menschen, die darauf achten, dass alles durchgeführt wird.

Diese Tools, Mitarbeiter und Prozesse arbeiten daran, Compliance-Verstöße zu erkennen, was Ihre Organisation vor potenziellen Katastrophen schützt.

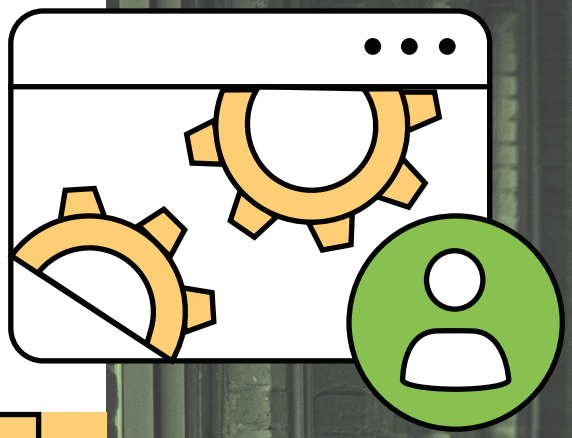
Cybersicherheit und Jamf

Als das britische National Cyber Security Centre seinen Leitfaden für **die Cybersicherheit** veröffentlichte, wendeten sich Organisationen, die diese neuen Anforderungen erfüllen wollten, an Jamf.

Weitere Infos

Wie kann ich in meiner Organisation mit dem Compliance-Management beginnen?

All das kann überwältigend wirken, aber wie bei jeder großen Aufgabe sollten Sie die größeren Segmente in kleinere aufteilen und auch um Hilfe bitten.



Hier sind einige Schritte, denen Sie folgen sollten, um richtig anzufangen.

1. **Stellen Sie sicher, dass alle zustimmen.** Ihre Organisation muss einem effektiven Compliance-Management-System zustimmen, und die Zustimmung muss auch ganz von oben kommen. Sammeln Sie eine Gruppe von Menschen, die diese neuen Prozesse in Ihrer gesamten Organisation durchführen können.

   Analysieren Sie die Compliance im ganzen Unternehmen – jede Art von Regulierung, branchenspezifische Vorschriften und wie diese Sicherheitsvorkehrungen Ihre Organisation, Ihr Personal und Ihre Kunden schützen.

2. **Führen Sie eine Risikobewertung durch.** Die Bewertung Ihrer Risiken führt Sie zum richtigen Compliance-Management. Letztlich geht es beim Compliance-Management darum, das Risiko zu reduzieren. Sehen Sie sich alle Ihre Systeme an – Ihre Werksanlagen, Ihre ethischen und juristischen Sicherheitsmaßnahmen, Ihre digitale Landschaft.

3. **Führen Sie einen Richtlinien-Audit durch.** Wenn Sie Ihre bestehenden Richtlinien mit der neuen Risikobewertung genau untersuchen, können Sie Bereiche finden, in denen Updates nötig sind.

Wie kann ich in meiner Organisation mit dem Compliance-Management beginnen?

Hier sind einige Schritte, denen Sie folgen sollten, um richtig anzufangen. (Fortsetzung)

4. **Schulung.** Stellen Sie sicher, dass alle Mitarbeiter wissen, warum die Compliance wichtig ist, ihren Platz innerhalb der Richtlinienstrukturen kennen und wissen, wie sie dazu beitragen können, Ihre Organisation zu schützen.

5. **Verstehen Sie, dass das nicht etwas ist, das man aktiviert und dann vergessen kann.** Richten Sie Systeme, Software und Auditverfahren ein, um Ihr Risiko kontinuierlich zu bewerten, Ihre Einhaltung von Vorschriften zu verfolgen und eventuell Lücken in Ihrem System zu finden. Aktivieren Sie automatische Berichte, Verifizieurngssysteme und klare Ansichten in mögliche problematische Stellen.

6. **Sorgen Sie dafür, dass alle verantwortungsvoll handeln.** Führen Sie wiederholt Schulungen durch und halten Sie Nachbesprechungen. Falls erforderlich, sollten sie deutliche disziplinäre Richtlinien für diejenigen einbeziehen, die gegen die Compliance verstoßen und sicherstellen, dass die Compliance in allen Bereichen aktiv und durchgängig durchgesetzt wird.

Unser Bereich: Geräte- und IT-Sicherheitsmanagement

Es gibt so viele Teile des Compliance-Puzzles, zu verfolgen, und das trifft vor allem auf IT und digitale Sicherheit zu.

Compliance ist kompliziert

aber Jamf kann helfen.

Wir bieten Unterstützung für Folgendes:

- **CIS-Benchmarks**
- **DISA-STIG**
- **NIST 800-171**
- CMMC (Eine neue Gruppe von Cybersicherheit Standards, die vom US-Verteidigungsministerium entwickelt wurden. Die **Cybersecurity Maturity Model Certification soll** Rüstungsunternehmen vor Cyberangriffen schützen.)
- **macOS Sicherheit und Compliance Projekt**

Und so schaffen wir das:

- Mit Apple Bestands-, Identitäts- und App-Lebenszyklus-Management.
- Durch Protokollansammlung, ein zentrales Datensystem, und SIEM
- Mit Verschlüsselung, Threat Defense und Risikobewertung für sowohl iOS, macOS als auch die Apps, die Sie darauf verwenden.
- Mit starken Datenrichtlinien und kontinuierlicher Überwachung von Datenlecks

Aber am wichtigsten ist, dass wir das mit unserem erstklassigen Support und dem umfassenden Wissen über Apple tun, und dass wir wirklich sicherstellen wollen, dass jede Organisation Apple Geräte erfolgreich einsetzt.

Kontaktieren Sie uns,
um zu verstehen, wie Jamf
Ihrer Organisation helfen kann
und testen Sie das kostenlos.

Testversion anfordern

Oder kontaktieren Sie Ihren
Apple Partner für den Einstieg.