Compliance management

for beginners

What is compliance?

Compliance simply means adhering to laws, health and safety standards, or data and security requirements.

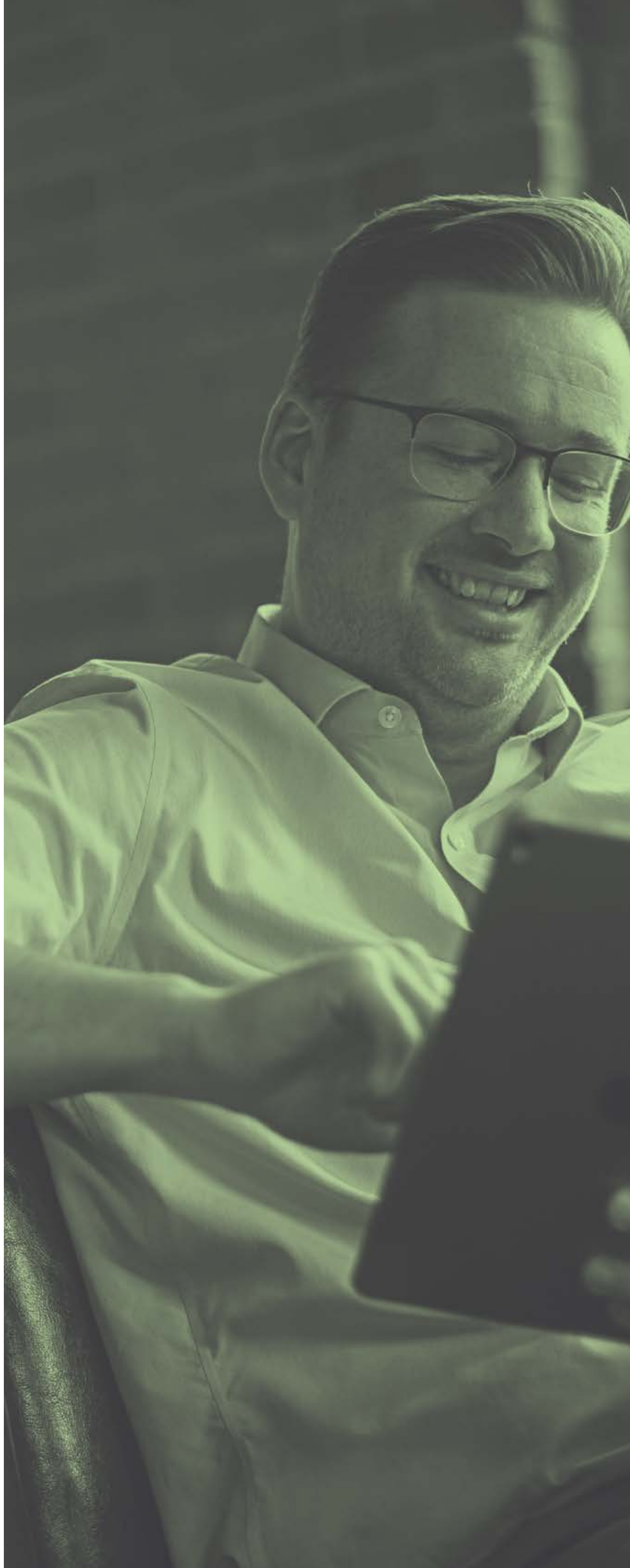
Sounds simple, right?

But wait.

Due to the specific nature of your organization, ‘compliance’ could mean a very different thing for you than the school down the street or the hospital across town. That’s why each organization should design its own compliance standards, and design systems for ensuring that your network of staff is able to adhere to them.

There are a few different types of regulation that require a compliance plan:

- **Legal regulations**, such as anti-discrimination, anti-slavery and anti-corruption laws
- **Industry standards**, such as quality standards or privacy standards
- **Security**, such as keeping a physical location safe, ensuring control over devices and maintaining data privacy
- **Organization-determined rules and responsibilities**, such as environmental impact or conduct requirements for vendors.



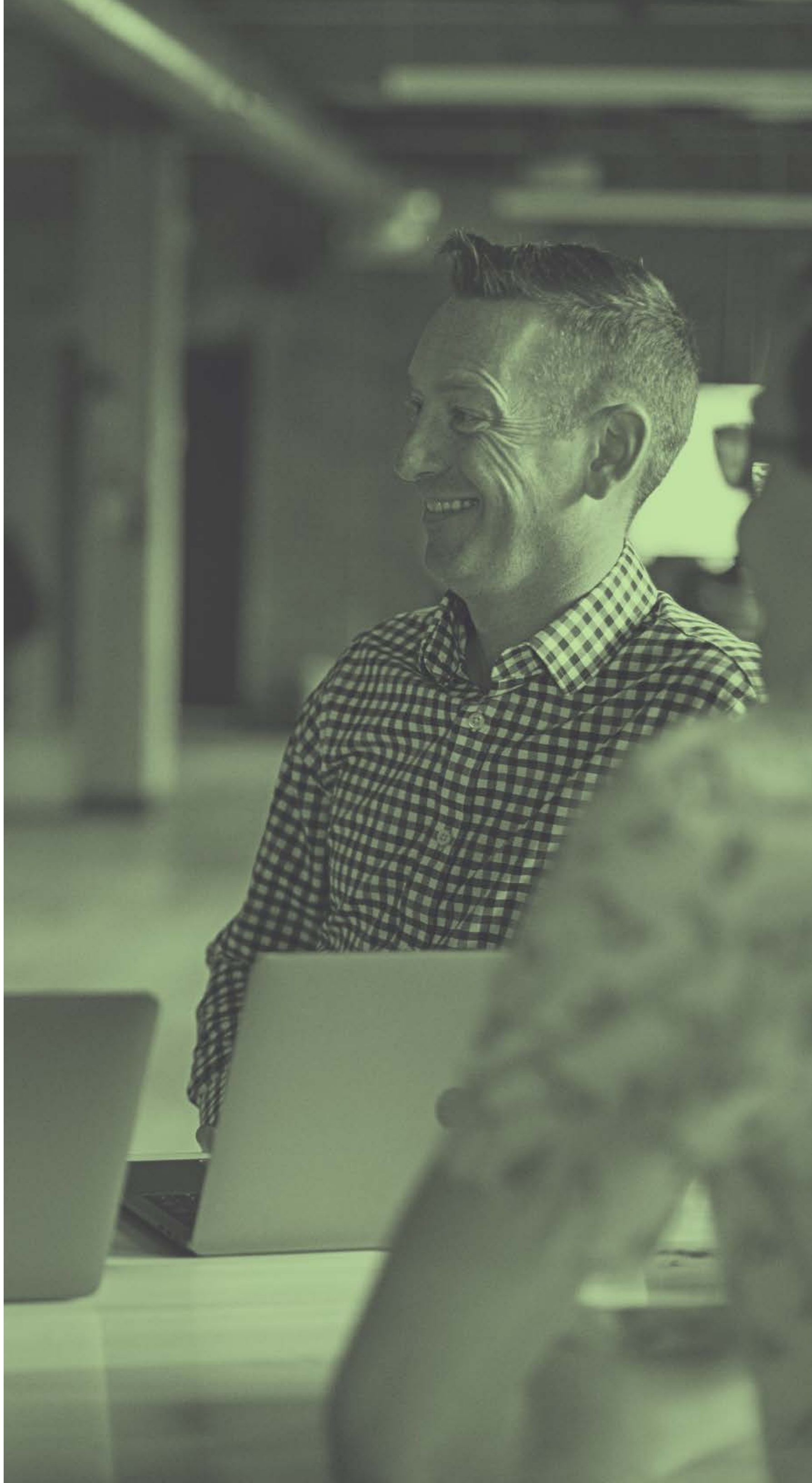
What is compliance?

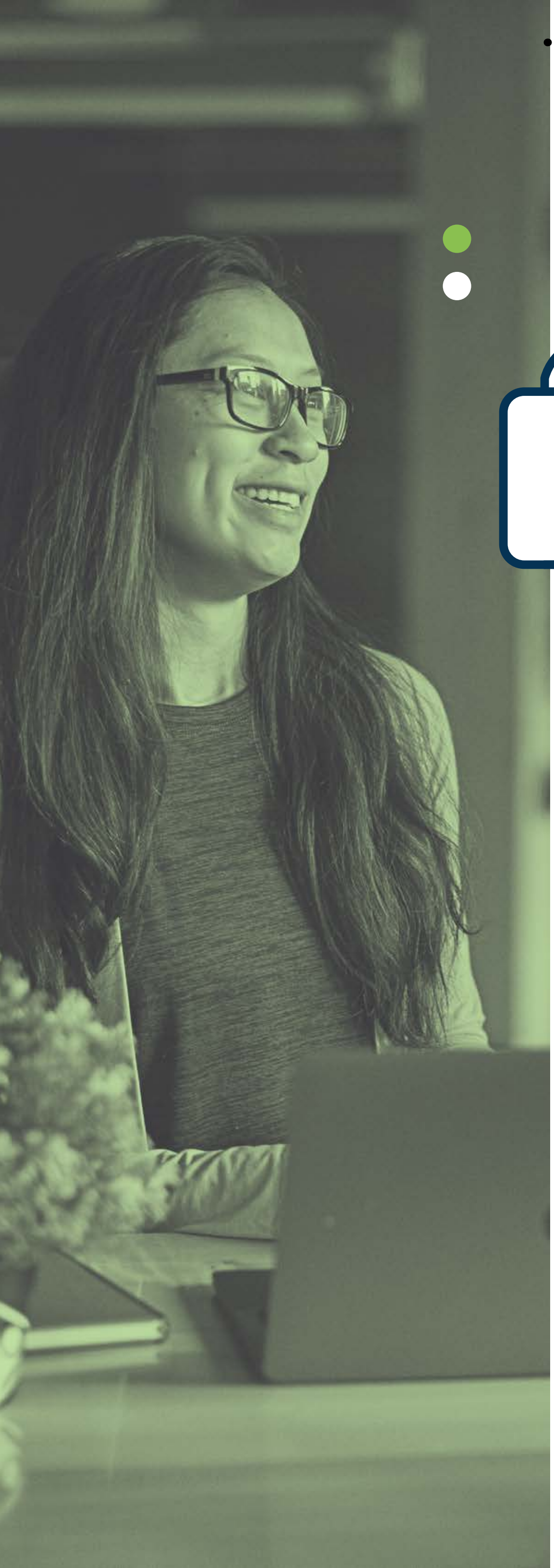
In each of these types of compliance areas, every organization must consider the impact on the organization as a legal entity; the impact on staff; and the impact on students, patients or customers.

And each industry has its own set of legal regulations, standards and security needs such as:

- **Healthcare** organizations must follow HIPAA
- **Higher education** institutions must adhere to FERPA
- **Financial institutions** must closely follow FDIC rules and regulations
- **Governmental institutions** must adhere to FIPS (Federal Information Processing Standards) and ensure that the three classification categories remain sacrosanct.

That's a great deal to consider and keep track of!
But it's also absolutely vital.





What can happen when companies ignore compliance?

We don't have to guess at what can happen; we have examples all around us, every day, of:

- Data breaches
- Data leakage
- Monetary loss: fines or settlements
- Loss of customers, accounts or jobs
- Loss of reputation

Here are just three examples that made international news:

1. A global retailer allowed 110 million customer's credit and debit card information to be stolen due to a vulnerability in a third-party app. Their reputation suffered greatly, and they paid $18.5 million in damages.

2. A large, well-known professional networking site paid a $1.25 million settlement for password leaking, and then more recently had a data leak of more than 700 million users' data, due to a vulnerability in its API. This impacted their reputation negatively and will likely cost them money as well.

3. Two large social networks, one in China and one in the US, had data breaches affecting 538 million and 533 million users respectively, exposing more than a billion email addresses and phone numbers.

In all of these cases, proper compliance procedures could have stopped these problems before they happened.

What is compliance management?

Compliance management is, well, how you manage your compliance.

It's the policies and procedures your organization enacts in order to ensure compliance in all areas, it's the digital tools you use to ensure compliance and — perhaps most importantly — it is the people who make sure that all of it gets done.

These tools, people and processes work to detect compliance violations, which protects your organization from these violations — and potential disaster.

Cyber Essentials and Jamf

When the UK's National Cyber Security Centre issued its **Cyber Essentials** scheme, organizations wishing to meet the new requirements turned to Jamf for help in implementing them.

Learn More

How can I get started with compliance management in my organization?

All of this can be overwhelming, but as with any large task you break down the larger pieces into smaller ones, and you ask for help.

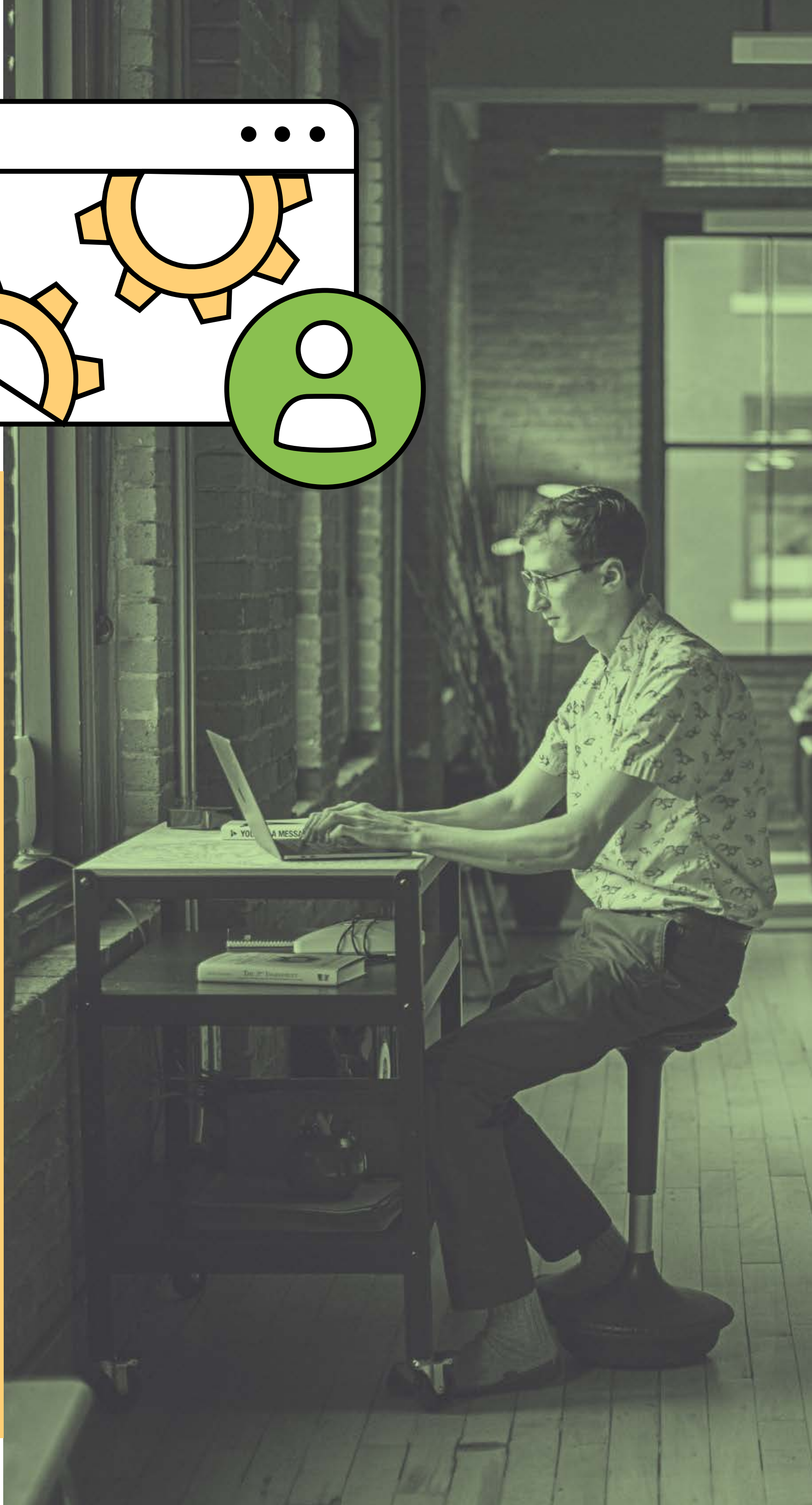
Here are some steps to follow that should get you off on the right foot.

1. **Ensure buy-in.** Your organization must be all on board for an effective compliance management system, and it must be from right at the top. Collect together a group of people who can enact these new processes throughout the entirety of your organization.

   Take stock of the entire compliance landscape for your organization: each type of regulation, regulations specific to your industry and how these safeguards will protect your organization, staff and clients.

2. **Conduct a risk assessment.** Assessing your risks will lead you to the right compliance management. The whole point of compliance management is, ultimately, to reduce risk. Take a look at all of your systems: your physical plant, your ethical and legal safeguards, your digital landscape.

3. **Conduct a policy audit.** Subjecting any existing policies to close scrutiny with your new risk assessment can expose any places where you need to make updates.



How can I get started with compliance management in my organization?

Here are some steps to follow that should get you off on the right foot. (continued)

4. **Educate.** Ensure that all staff understand why compliance is important, their place within the policy structures and how they can and must contribute to keeping your organization secure.

5. **Understand this is never a 'set it and forget it.'** Put systems, software and auditing procedures in place to continually evaluate your risk, your adherence to regulations and where possible gaps in your system might arise. Equip yourself with automated reporting, verification auditing systems and clear sight lines to any possible problem areas.

6. **Keep everybody accountable.** Continually educate and also follow up. If necessary, include clear disciplinary guidelines for those who damage your compliance and ensure that your compliance in all areas is actively and consistently enforced.

Our wheelhouse: device and IT security management

There are so many pieces to track in the compliance puzzle, and no more so than in information technology and digital security.

Compliance is complicated

but Jamf can help.

We offer assistance with:

- **CIS Benchmarks**
- **DISA-STIG**
- **NIST 800-171**
- CMMC (A new set of cybersecurity standards developed by the Department of Defense, the **Cybersecurity Maturity Model Certification program**, created to protect defense contractors from cyber attacks.)
- **macOS Security Compliance Project**

And here's how we do it:

- With Apple inventory, identity and app lifecycle management.
- With log aggregation, a central system of records and SIEM
- With encryption, threat defense and risk scoring for both iOS, macOS and the apps you use on them
- With strong data policies and continual data leakage monitoring

But most importantly, we do it with our world-class support and extensive knowledge of the Apple landscape, and with our sincere desire to ensure that every organization succeeds with Apple.

Contact us to understand how Jamf can help your organization and try it for free.

Request trial

Or contact your preferred Apple reseller to get started.