eBook

jumpcloud™

The IT Manager's Guide to Data Compliance Hygiene

Ace Your Audits with Less Stress

Introduction

Mindset — it's often the difference between a smooth journey (with a few bumps along the way) or a stressful sprint to the finish line (with many twists and turns).

This applies to everything from menial tasks to large-scale initiatives. Mindset shapes not only how you think about things, but how you go about accomplishing them.

As an IT manager, your mindset around why compliance matters informs your daily thoughts, feelings, and actions that will make or break future audits. Translation: you can view audit preparation in one of two ways:

1. A hassle to deal with before moving onto "what really matters" or
2. An incentive to practice strong security hygiene that keeps everyone safe.

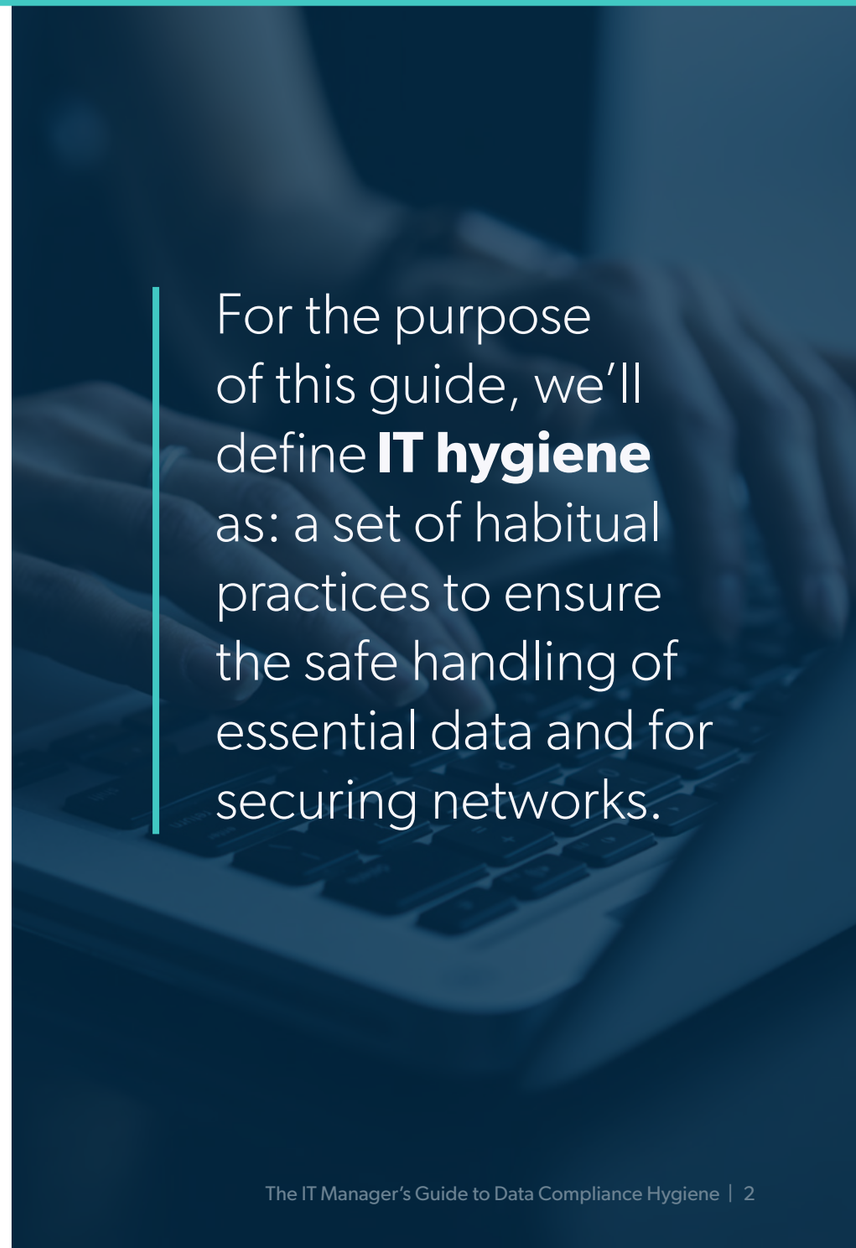
If you have downloaded this guide, you are probably spearheading the IT audit process for a startup or small-to-medium-sized enterprise (SME) for the first time. Or maybe you're an old pro looking to see what else you could be doing. Either way, we invite you to hit "pause," take a deep breath, and exhale.

You don't have to be perfect to pass your audit, and we can pretty much guarantee there is no such thing as 100% compliance at all times. This is why we recommend prioritizing the right actions throughout the year to ensure optimal results rather than just focusing on the operations of the audit itself. And that means increasing emphasis on the things you know matter, but may avoid prioritizing; in other words, **IT hygiene**.

We don't need to quote the latest cybersecurity breach statistics for agreement that security hygiene is about more than avoiding fines. But you may find it surprising that cyber attacks on SMEs have increased by approximately **400%** over the past year. Consistent security hygiene is essential to reducing the likelihood of your brand name becoming the next newspaper headline.

This guide will review several IT hygiene practices worth automating year-round to facilitate smoother audit processes. It will also explore the relationship between faster prep times and consolidated toolkits/systems.

After reading, you can expect a better understanding of how (and why) to conduct internal audits, which preparatory action steps save time, and what to expect during official audits.



For the purpose of this guide, we'll define **IT hygiene** as: a set of habitual practices to ensure the safe handling of essential data and for securing networks.

The Benefits of IT Hygiene

At first glance, it may not seem like IT hygiene is related to audit preparation. The latter involves gathering lists of data, securing an auditor, providing documentation, explaining control failures, and making remediation plans within a brief period of time.

The former refers to following through on best practices 24/7/365. But much like a runner shouldn't begin training a week before a marathon, an IT manager shouldn't start practicing IT hygiene right before their next audit! In addition to facilitating smoother compliance experiences, prioritizing IT hygiene provides the following benefits:

1 Identifies Inefficient Processes

Inefficient processes slow down operations, creating unnecessary bottlenecks. Data regulations mandate IT managers to discover opportunities for more efficient processes, procedures, and tools.

For example, imagine a pizza delivery firm that receives customer orders from one software, customer reviews from another, and order statistics from yet another.

An IT manager that prioritizes IT hygiene would seek opportunities to eliminate redundancies and unify data collection for more accurate reporting. Typically, this would involve switching to a software service that provides all these functions in its offerings.

This unified data collection makes it less likely that there will be a breach by reducing the overall attack surface and focusing security efforts, and makes data audits easier. It also makes the marketing department, which looks at the data for business reasons, more efficient because they have to do less copying and pasting from one application to the next when reviewing their marketing strategies.

Alternatively, managers who practice lackluster IT hygiene often find themselves switching between many misconfigured applications, which often increases vulnerabilities. In addition, purchasing multiple single-point solutions can be hard on the budget.

2 Reduces Security Vulnerabilities

Minimizing security vulnerabilities is the whole point of compliance, but it's worth emphasizing. Cybersecurity breach incidents scaled new heights in 2021.

According to the Identity Theft Resource Center (ITRC), data breaches increased more than 68 percent from 2020 to 2021. To make matters worse, an increasing amount of data incidents involve sensitive information, such as Social Security numbers.

The solution, of course, is data hygiene. According to the Microsoft Digital Defense Report, basic security hygiene still protects 98% of attacks. We'll call out the most crucial security hygiene practices you can take further down in the guide.

68%

Data breaches increased more than 68% from 2020-2021

The Benefits of IT Hygiene

3 Helps Avoid Penalties or Legal Trouble

Failing to follow through with mandatory IT hygiene regulations can cause serious trouble. According to The True Cost of Compliance with Data Protection Regulations study by the Ponemon Institute, non-compliance with leading cybersecurity standards costs more than twice as much as maintaining compliance.

Following data-compliant practices isn't always "easy peasy." But it's far more convenient and less expensive than paying legal fees, fines, or even worse penalties.

Of course, it isn't only cookie violations and personal information mishandling that can get a company into legal trouble. Failing to take adequate steps to prevent security breaches can result in millions in fines. British Airways knows a lot about that one.

> "…non-compliance with leading cybersecurity standards costs more than twice as much as maintaining compliance."

4 Minimizes Costs to Stay Compliant

Staying compliant is expensive; your organization may spend anywhere from a few thousand to hundreds of thousands of dollars on direct and indirect costs annually.

Totals vary based on the amount of employees, regulatory requirements, and data under your care. If your business processes credit card transactions, you're likely following the **Payment Card Industry Data Security Standard** (PCI DSS).

Gary Glover, vice president of assessments at SecurityMetrics, says annual compliance costs for PCI DSS range from $10K to $70K depending on the number of transactions processed. This includes expenses associated with updating policies, replacing old technologies, training employees, penetration testing, and on-site audits.

Alternatively, a typical SOC2 audit ranges from $25K to $39K . Failing to practice IT hygiene throughout the year means you're more likely to accrue additional expenses to "get it together" in time for your audit. Common costs accrued include exorbitant consultant fees, suspended business partnerships (due to failing grades), and astronomical regulatory fines.

5 Secures Business Partnerships

Have you ever heard the phrase "excellent practices breed excellent partnerships?" Probably not because we just made it up. But it's true — being IT-compliant silently communicates that your organization is up-to-date with the latest trends, technologies, and practices.

In other words, good cybersecurity habits forge a bond of trust between companies and prospective business partners. A higher level of trust translates to more referrals, improved vendor relationships, and more potential customers.

Highly regulated industries like healthcare, government, and banking are especially vulnerable to losing partnerships due to non-compliance. In addition, most enterprise-level companies require the minimum of a SOC2 and ISO27001 before they will even consider doing business with your organization. And, if that weren't enough, you will have a tough time securing cyber insurance which also impacts who will and won't work with you!

For the remainder of this guide, we'll connect the dots between the things you must do to satisfy data compliance audits and the IT hygiene best practices that support them.

Remember: audits may seem burdensome, but they provide an essential foundation for organizations to implement proven cybersecurity measures that keep precious data safe — standards that contain both proven and cutting-edge methods to ensure security.

Changing the Way You View Compliance

Have you ever met an IT manager that woke up one morning and said, "Hey, today is a great day for compliance! Wouldn't putting systems in place be fun?" No, we haven't either.

No one has ever described preparing for a compliance audit as "fun." Especially startups and SMEs still learning the ropes. Limited resources, knowledge, and expertise can stall forward momentum to a grinding halt.

Furthermore, it's not unusual for busy executives to assign compliance initiatives to IT managers on short notice. Depending on how many regulations your organization must meet, it may seem like various deadlines are popping up all the time! The good news is once you know what to expect, audits begin to feel more like opportunities to prove operational excellence — which is the entire point — instead of burdensome hurdles.

Michelle McGough, Principal Product Manager at JumpCloud, has led compliance initiatives for several types of organizations throughout her career — from spearheading internal audits for a "unicorn" SaaS company to investigating compliance complaints, concerning hundreds of thousands of devices, as a federal government supplier. She's no stranger to the "dreaded" auditing process and says the biggest reason many IT leaders dread audits is fear of the unknown.

The good news is that assumption isn't always true. There will always be devices that fail to meet ideal standards for one reason or another. Even the most forward-thinking IT managers encounter situations where failure is inevitable. For example, the larger the organization, the more likely you are to have devices being repaired and deployed at any given time.

The important thing is to:

A | document the reasons behind the exceptions to standard operating procedures and

B | show proof of the actions you will take to remedy them.

Thus, audit success ultimately comes down to having the right management toolkits in place to demonstrate you have clearly understood the definitions and are using the right controls.

> **"I think that they feel almost like they're in court," she says. "It's a recorded conversation, and there is a lack of knowing what's going to happen. There's also a sense that if anything is wrong it means the business hasn't been practicing good compliance at all."**
>
> *— Michelle McGough, Principal Product Manager, JumpCloud*

What is an IT Compliance Audit?

Before diving into our best practices, let's familiarize ourselves with some useful terminology:

Compliance Audit

Compliance itself is a practice. Alternatively, an IT audit is a protocol to establish that organizations are practicing the actions they say they are in accordance with compliance standards, regulations, and laws. Therefore, a compliance audit is an independent review process pursued with the intention of verifying agreed-upon best practices. Both external certification bodies and internal stakeholders conduct audits.

IT Audit

A specific type of evaluation concerned with an organization's cybersecurity tools, practices, and policies.

Internal Audit

An in-house assessment of an organization's IT infrastructure, policies, procedures, and personnel. Auditors review IT systems and controls, interview personnel, and observe processes to help identify opportunities for improvement.

External Audit

An audit typically conducted by a third-party auditor to verify an organization is compliant with IT best practices, laws, and regulations. External audits are sometimes required by law or contractual agreement. For example, many companies that process credit card payments are required to comply with the Payment Card Industry Data Security Standard (PCI DSS). In other instances, organizations conduct external audits to obtain a necessary "Big Four" endorsement that is crucial to forging high-level partnerships.

Personal Identifiable Information (PII)

PII is any data that could potentially identify a specific individual. This information includes a person's name, address, date of birth, Social Security number, and even biometric data.

Controls

Controls are systems, processes, or policies put in place to mitigate breaches and undesirable circumstances from happening.

While you will likely encounter many other "fun" vocabulary words on your compliance journey, the above-mentioned are the basics you should know.

Common Data Compliance Regulations

Depending on your organization's unique industry, region, and size, you may be asked to comply with one or several regulations.

Compliance regulations fall into three categories:

General standards apply to a wide list of organizations, regardless of their location or industry.

Examples

National Institute of Standards and Technology (NIST) Special Publication 800-53, ISO 27001.

Industry regulations apply to specific industries or organizations that handle specific types of data.

Examples

Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes–Oxley (SOX) act.

Regional regulations apply in particular countries, regions, or US states.

Examples

EU General Data Protection Regulation (GDPR), UK Data Protection Act, California Consumer Privacy Act (CCPA), New York State Department of Financial Services (NYDFS) Cybersecurity Regulation, and FCA Operational Resilience.

Next, let's look at some of the most common standards and regulation requirements.

HIPAA

The Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA, is a federal law that establishes standards for the privacy and security of protected health information. HIPAA applies to any entity that handles protected health information, including healthcare providers, insurers, and in some cases, schools.

The law requires these entities to take steps to safeguard this information from unauthorized access, use, or disclosure. In addition, HIPAA gives individuals the right to access their own health information and control how it is used and shared.

SOC Type I / Type II

Organizations often provide services to other companies (called "user entities") that can impact the latter's financial and cloud computing reporting. User entities' auditors require Service Organization Controls (SOC) reports to be assured that the controls surrounding an organization's services are designed and operate effectively.

The SOC 1 report, also referred to as the SSAE 18, has a financial scope and addresses the service organization's controls that are applicable to an audit of a user entity's (customer's) financial records. Based on the 5 trust categories outlined by the American Institute of Certified Public Accountants (AICPA), a SOC2 report examines a service organization's operational and compliance controls. It was formed partly due to increased cloud computing and business function outsourcing.

SOX ITGC

The Sarbanes-Oxley Act (SOX) is a U.S. federal law enacted in 2002 in response to several high-profile corporate scandals. SOX applies to publicly traded companies, foreign companies, and wholly-owned subsidiaries doing business stateside.

Though the act doesn't enforce specific information technology protocols, it absolutely impacts organizational technology systems. For this reason, any organization aiming for high-velocity growth will have to participate in this audit at one point or another.

The act contains several provisions designed to improve financial disclosure and corporate governance. For example, SOX sections 302, 404, and 409 require corporations to keep accurate financial records and have internal controls to avoid fraud. The act also imposes stiff penalties for companies that engage in fraudulent activities, including fines and jail time for fraudulent executives and auditors.

ISO 27001

ISO 27001 helps enterprises protect confidential data. The standard addresses risk assessment, management, and physical and technical security controls. The 27001 standard doesn't require specific security measures, but its companion code ISO/IEC 27002:2005 gives a shortlist of controls to examine.

ISO 27001 helps firms manage people, procedures, and technology for information security. Although not obligatory, cloud computing companies, financial institutions, and telecom services often implement ISO 27001 standards in order to follow security best practices.

Common Data Compliance Regulations

CIS Benchmarks

Center for Internet Security benchmarks are best practices for system configuration. Each recommendation refers to one or more CIS controls to strengthen cyber defense. NIST Cybersecurity Framework (CSF) and NIST SP 800-53, ISO 27000, PCI DSS, HIPAA, and other standards are mapped to CIS controls.

Internationally known CIS criteria guard against cyberattacks on IT systems and data. They assist hundreds of businesses in establishing a secure baseline configuration.

PCI DSS

As mobile and touchless payment continue to grow in popularity, credit card data breaches remain at the forefront of cybersecurity conversations. On-prem and self-hosted SaaS organizations alike must follow the Payment Card Industry Data Security Standard (PCI DSS) to protect cardholder data. PCI DSS applies to all organizations that process, store, or transmit card information from major card schemes.

The PCI Security Standards Council manages the standard, an organization founded by major credit card companies such as Visa, Mastercard, Discover, and American Express. Though simple upon first glance — it only includes 12 requirements — a closer look reveals a whopping 251 sub-requirements spanning aspects of device, network, and processor management.

It's worth emphasizing that PCI sub-requirements are constantly shifting so make especially sure to always double-check the latest guidelines.

GDPR

The General Data Protection Regulation (GDPR) is a regulation of the European Union (EU) that strengthens and builds on the EU's current data protection framework. The GDPR sets out strict rules about how personal data must be collected, used, and protected.

It imposes a high level of legal liability if the organization's security gets breached. The GDPR applies to any company that processes or intends to process the data of individuals in the EU, regardless of whether the company is based inside or outside the EU.

Essential Eight (8)

The Essential Eight is a set of eight security strategies developed by the Australian Cyber Security Centre (ACSC). They can help protect organizations from the vast majority of cyber-attacks if implemented. The Essential Eight is not a silver bullet but represents an essential baseline for cybersecurity. The Essential Eight strategies prevent, limit, and provide data recovery options against cyberattack.

CMMC

The Cybersecurity Maturity Model Certification (CMMC) is a new cybersecurity certification mandated by the Department of Defense in the United States (DoD). It's a collection of requirements for defense contractors to keep, handle, and transmit Controlled Unclassified Information (CUI). The CMMC 2.0 framework has three levels, each with increasingly strict standards. To be accredited, DoD contractors at all levels of the supply chain must meet all requirements at their respective levels.

Cyber Essentials and Cyber Essentials Plus (in the UK)

The UK Government's Procurement Policy requires suppliers bidding for government contracts to achieve certification in Cyber Essentials or Cyber Essentials Plus. The mandate is part of the government's strategy to enhance the country's defenses against cyber-crime.

Cyber Essentials includes a lightweight self-assessment and internally vulnerability scan that demonstrates the practice of five essential controls: secure configuration, patch management, malware control, access control, and boundary firewalls. Alternatively, Cyber Essentials Plus requires an external vulnerability scan and an on-site assessment.

> Would you believe this list includes only a fraction of regulations governing data compliance? Unfortunately, there are a thousand road signs and potential sources of confusion on the road to compliance.
>
> The good news is that security regulations and standards often overlap in requirements. So long as your team consistently minds data hygiene best practices, consolidates tooling, and emphasizes ongoing security awareness training, you can handle multiple mandates as needed. This brings us to our next topic of discussion: why continuous compliance with data regulations can be challenging.

The Challenge of Adhering to Compliance 24/7

Several organizations run afoul of data protection standards, and it's easy to understand why.

Data compliance requires adhering to several overlapping guidelines that range from **disclosing how collected data is used** to restricting access to sensitive information to **fixing security vulnerabilities** to **ensuring the accuracy** of information.

But the real challenge lies in meeting these obligations in the context of having to comply with multiple regulations at once. Let's discuss some common challenges you may face when implementing compliance regulations and how to confront them:

1 Long Review Periods

One of the most nerve wracking aspects of data compliance audits is timing. Take SOC 2 Type II for example. It involves a two to three month remediation period followed by a three, six, or 12 month observation period. The length of the observation period is up to your organization.

During this period, auditors can conduct interviews with stakeholders, request evidence of controls, and assess compliance at random. Unfortunately, this means they may happen to choose a nontypical day with a high number of control failures.

In such instances, it's your responsibility to explain what's going on. For example: *here is the list of our devices, and here is the list of items that aren't compliant. We have tickets open on 10 devices and a handful of devices that were recently deployed for new hires yesterday*

2 Unclear Control Guidelines

Regulatory agencies provide little guidance toward selecting and defining controls. While certain guidelines leave no room for misinterpretation (e.g., employ multi-factor authentication), others provide significant leeway on the best course of action for achieving results.

Even the **AICPA** is a bit vague when it comes to providing instructions for SOC 2. With dozens of controls spanning multiple security avenues, it's easy to get lost in the weeds. Audit workflow software is one way to expedite the process.

In addition, the JumpCloud Open Directory Platform provides recommended policies that you can turn on with the flip of a switch. The platform's customization makes it easy to automate the most common controls and hygiene standards you need to achieve compliance.

The Challenge of Adhering to Compliance 24/7

3 Competing Regulatory Requirements

Sometimes the problem isn't "not knowing what to do," but navigating seemingly conflicting standards and regulations. Just ask Idan Mashaal, JumpCloud Senior EMEA Solution Consultant and Israel country manager.

During his time as employee no. 5 at Plus500, Idan confronted many unexpected challenges while managing requirements from multiple countries including the UK (FCA), Australia (ASIC), Cyprus (CYSEC), and more.

"In one particular instance, the GDPR said we needed to allow users to be forgotten, but the financial regulations said I needed to store the information for seven years, " he said. "So, we were in a debate between the law and the European Union, which dictated a 50 million euro fine, and the license that will allow me to make money."

In addition, the GDPR only applies to the EU, which begs the question: should the organization apply the regulatory standard universally (at the expense of global business) or should it create a system for separating businesses outside of the EU?

Ultimately, Idan realized "the right to be forgotten" isn't synonymous with the "right to be deleted." The solution was to "forget" who the user was as a person while still keeping the data intact. This is just one example of the many types of unexpected situations you may encounter when becoming compliant.

4 Balancing Usability and Regulatory Compliance

Balancing data compliance controls with workflow efficiency isn't always easy. In some cases, regulations present unrealistic parameters that defeat their purpose. For example, say one regulation requires the enforcement of a lock screen mechanism every 10 minutes.

But your Research & Development (R&D) Department says that any locking mechanism under 15 minutes interferes with their daily processes. This is just one of many small, but significant challenges that can occur when balancing controls with user experience.

Admins are often faced with answering a difficult question: *Do we run the business most effectively or most securely?*This unintentional catch-22 can make it even more difficult to find effective solutions that achieve both ends.

Perspective Shift

As an IT manager, you can and are expected to solve problems in innovative ways. You can ideate creative workarounds as you build towards compliance so long as you can a) provide the reason behind the control failure and b) provide documentation of proposed remediation.

In such instances, your auditor will check back in 30 days. As long as you have followed through with your remediation plans, and demonstrated intelligent thought in following guidelines, you're in good shape.

Remember: auditors aren't pencil-pushing enemies analyzing rows of data for breakfast! They are supportive professional partners who possess valuable insights to help you succeed. The more transparent you are from the beginning, the better equipped they are to propose unique solutions to your problems.

Ultimately, being compliant means playing by the rules, even when it's difficult to do so. Work with your auditor to seek solutions to whatever makes it tough to follow a particular regulation, rather than assuming nothing can be done.

Let's dive into how to make compliance a bit easier in our next section.

7 IT Hygiene Best Practices to Follow

Whether you're a startup or an enterprise-level company, the best practices for achieving compliance are the same. The only difference is the amount of rigor required.

Audits happen regularly, and regulations change frequently. Translation: you must consistently carve out time to review and improve your existing security practices.

You can think of IT hygiene as your team's standard operating procedures that work harmoniously as part of your overall compliance strategy. A compliance strategy is a set of internal policies and procedures that will help your organization stay compliant.

Once your compliance strategy is complete, it's essential to assign team members responsible for implementing the various parts. Remember, IT compliance is a team effort that involves the contribution of many individuals outside of the IT department. Below are seven best practices worth following:

1 Monitor Your Unique Regulatory Requirements

Before setting out to improve your compliance posture, figure out which standards are mandatory and which ones aren't. Pay attention to obligatory and non-obligatory regulations, as both provide an organization with the benefits we discussed above.

For example, while HIPAA compliance is non-negotiable for health organizations, ISO 27001 implementation is voluntary. Nonetheless, according to the ISO Survey 2018, the demand for ISO certification grows by the year. In addition, you must also determine where the requirements of a specific regulation apply to your organization.

If you're uncertain about which audits you need to pass, consult with someone who has already "been there, done that" in your industry, trade, or supply chain. An experienced auditor will also know which standards and regulations your type of organization must follow.

Smaller SMEs won't have cybersecurity staff or even access to dedicated lawyers, at least not those practicing cyber. I'd suggest that you consult with your industry, trade, supply chain, and/or regional peers or simply ask your auditors on the regulations you might be subject to.

You can also analyze the data your organization handles to figure out which requirements it's subject to. *Usually*, IT compliance focuses on three types of data:

- **Personally identifiable information:** Any information that relates to an identifiable person: name, home address, date and place of birth, biometric records.
- **Financial data:** Credit card numbers, data on income and expenses, financial reports of an individual, organization, or any other entity.
- **Protected health information:** Results of medical examinations, information about health care plans, and any medical records linkable to a specific person.

In addition, pay attention to the privacy standards and remember that laws such as the GDPR and the 2019 Online Privacy Act contain web/cookie data regulations. Hence, if your business handles customer cookies, you'll be better off obtaining permission before retrieving necessary cookies and letting your clients' have full disclosure on how their data is used.

7 IT Hygiene Best Practices to Follow

2 Appoint a Data Protection Leader

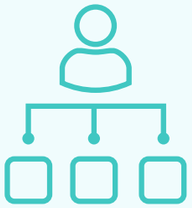
Large enterprises often hire internal **data protection officers** (DPOs) to oversee data protection measures and ensure the department is responsible for meeting them. If you're a startup or SME, you probably don't have the budget or bandwidth for a full-time DPO yet.

But that doesn't mean you can't recruit an internal data protection leader to drive your compliance efforts on the side. Both the GDPR and PCI DSS require an organization to designate an employee who is responsible for compliance. Your compliance champion should make an effort to:

- **Increase knowledge of cybersecurity legislation.** Having an expert on the team translates into being able to develop data-compliant policies and procedures for data handling. It also means that staff can be better and continuously trained on data protection best practices. In addition, the project driver can act as a resource for employees who have questions about the organization's data protection practices.
- **Regularly monitor IT compliance statuses.** While other staff focus on their roles between audits, your data protection leader can perform data protection impact assessments (DPIA), track changes in regulations, and check whether current security controls are in tune with current data-protectionist standards.
- **Quickly respond to breaches.** In the event of a security breach, the data protection leader should have a plan in place for doing damage control, notifying affected parties, and reporting the breach to authorities and clients. Fast response times mitigate consequences and reduce fines.

It's worth mentioning that the conflict of interest requirement doesn't mean a DPO can't hold other roles within the company. Still, such a role must not be one that can involve making decisions that might mean data protection taking the back seat while business considerations ride shotgun.

However useful a DPO or data protection leader may be, it's important to remember that a single person can't make an organization compliant. This person will require support from company management and the authority to improve existing security controls and policies, reconfigure existing software, and deploy new software.



It's important to remember that a single person can't make an organization compliant.

3 Conduct a Risk Assessment and a Self Audit

A **risk assessment** identifies and analyzes security risks your organization might face.

During a risk assessment, it's important to identify:

- cybersecurity risks and threats to your organization
- assets that are critical to your organization and are subject to compliance regulations
- your current level of protection, as well as the weak and strong points of your defenses

A self-audit has a lot in common with a risk assessment: it's an evaluation of implemented security controls. But unlike a risk assessment, a self-audit helps you evaluate your current compliance level and identify gaps in data protection. It also prepares your employees for a real IT audit.

Most startups begin conducting quarterly self-audits no sooner than their board of directors tell them to "get on the ball." No matter the size of the organization, most internal audits include the same basic steps as shown below.

The one drawback to self-audits is their high cost, both in terms of money and time. However, discovering gaps in cybersecurity during an actual audit has an even higher cost: failing the audit and starting over!

Below are the three basic steps of conducting an audit:

- **Gather lists of assets:** Assets refers to all relevant IT-related stuff (i.e., devices, devices with full-disk encryption, users etc.). This typically comes from a master IT asset management platform. Pro Tip: Prioritize maintaining a central source of truth.
- **Identify the gaps:** Upon comparing your lists, you may be surprised to find several assets listed within the master database are unaccounted for in the lists coming from your IT tools. Answer questions like:*Where are these items? Why aren't they following protocol? Do we have devices out for repair?*
- **Fix the outliers:** Once you have identified non-compliant assets, you're ready to make a remediation plan. Auditors are real people who understand reasonable exceptions. Taking action to demonstrate reduced risk however you can and explaining the reasons behind any outliers with screenshots is satisfactory.

Unfortunately, you're never going to have everything you need in one place for compliance. There are simply too many factors you must take into account. But you can still save time and energy by consolidating tooling wherever possible.

7 IT Hygiene Best Practices to Follow

4 Fix Missing Controls

OK, you have finished conducting your risk assessment and self-audit. You now know what policies, practices, and technical controls to implement for a passing grade. At this point, it's time to take action and fix any oversights you found.

The good news? Requirements of common regulations, standards, and laws overlap in many areas. It's likely that some of the elements you fix today will make things easier for your team in the future. For example, most data mandates require using tools for identity management, access control, user activity monitoring, and breach notification.

While it's beyond the scope of this guide to delve into comprehensive controls, below are **nine of them** worth following year-round. You will find these general protocols as requirements in many different types of regulations.

There are many other aspects of data compliance hygiene that we can't cover in the scope of this guide. But by following best practices in online security, physical security, and incident response, you've got no need to be jittery about that upcoming compliance audit.

Unifying your stack with the JumpCloud Directory platform can also relieve the stress that comes with tool sprawl. JumpCloud combines Linux, Windows, Mac, and iOS devices behind one pane of glass for convenient heterogeneous device management. In addition, JumpCloud also handles identity and access management (IAM), and Zero Trust security elements like single sign-on (SSO) or multi-factor authentication (MFA).

Here are some of the controls we recommend prioritizing always:

Full-Disk Encryption:

Full-disk encryption (FDE) is a simple way to ensure data remains inaccessible without an authentication key should a device become lost or stolen. Every organization should prioritize FDE regardless of regulatory requirements.

Anti-Virus Software:

Like the battle between good and evil, cybersecurity is a classic depiction of infinite warfare. New security threats always emerge, and so must the measures to combat them. This means admins should run the latest versions of antivirus software on company endpoints at all times.

Breach Notification:

Notifying affected individuals and regulators of a data breach helps mitigate damages caused by unauthorized access or disclosure of personal information. In addition, breach notification gives individuals the opportunity to beef up protection from future identity theft and scams.

Identity Access Management:

Use Identity and access management (IAM) solutions to control who can access, view or modify sensitive information. IAM measures aid in compliance with data privacy regulations, such as the General Data Protection Regulation (GDPR). Platforms like JumpCloud also automate audit trails so admins can easily prove policy adherence.

MDM Patch Management:

The global shift toward remote work and the adoption of Bring Your Own Device (BYOD) policies necesitate continual patch updates. Manual patching reduces IT worker productivity and increases the likelihood of overlooking outlier devices. Automated patch management saves time and increases accuracy.

Multi-Factor Authentication (MFA):

MFA is one of the easiest controls to implement that can yield extremely high dividends. Enforcement can range from requiring biometric data in addition to a password, to asking for the user's maiden name and considering what role the user holds in the organization.

Naming Conventions:

Savvy admins adopt naming conventions because it helps them find requested data lightyears faster. It also facilitates carrying over information when installing other management solutions. Establishing distinguishable names for device classes and individual devices is simply good hygiene. Don't name every device "Company XYZ's Macbook!"

Password Security:

Strong password security requires the implementation of several policies. Password complexity, anti-keylogging measures, and anti-phishing measures are all essential components of good data hygiene.

Data Backups:

Backing up data is like stashing cash for a rainy day. No one wants a system failure or data breach, but it's essential to prepare for the unexpected. Store encrypted data backups in a secure location unaccessible to unauthorized individuals.

7 IT Hygiene Best Practices to Follow

5 Setup IT Audit Trails

Maintaining a clear **audit trail** is essential to acing any audit. An IT audit trail is a set of records that depict any activities with sensitive data, databases, applications, or parts of your infrastructure. It allows IT compliance auditors to examine how your employees handle sensitive resources and assess that you have been doing what you said you would.

Audit trails can be manual or electronic so long as they act as documentation and proof of compliance. Security policies and processes (like data retention and document control) significantly manage audit trails.

Digital audit trails offer a number of advantages over their analog counterparts. For one, they are much harder to manipulate or tamper with. This can be valuable in situations where fraud or misuse is suspected. Additionally, digital audit trails are usually more accurate and up-to-date than analog records. This can save time and money that would otherwise be wasted on trying to track down missing or outdated information.

Finally, digital audit trails provide a more complete picture of your compliance posture at any given moment. This is because they are more readily accessible in real time. Logging an audit trail is also useful for security monitoring and incident investigation. You can track any action inside your protected environment using generated logs, identify security incidents, and assess threat sources.

Maintaining a clear audit trail is essential to acing any audit.

6 Automate Compliance-Related Activities

For now, there isn't a workaround for the manual effort necessary for some compliance audit activities. Reviewing policies, investigating security incidents, and cooperating with certification bodies takes time.

But thankfully, the vast majority of activities that go into making an organization data compliant can (and should) be automated. Automation tools help reduce compliance overhead, save time preparing for the audit, minimize the risk of human errors, and improve the overall efficiency of your IT operations.

Automation is especially helpful for large organizations that have to pass several IT compliance audits annually. It ensures your team performs tasks in the same manner each time.

While it's not possible to automate everything, prioritize automating what you can. The time it takes to do the upfront work is nothing compared to the long-term dividends of finding exactly what you need when you need it later. And, of course, you will sleep better at night knowing your organization's data is safe and sound.

> **JumpCloud's Directory Platform** provides a suite of tools that can help you automate many of the tasks associated with data compliance. With JumpCloud, you can manage passwords, users, events, automate security patches, and lots more all from one dashboard.

Several different ways to automate compliance-related activities exist, including:

Password Management: Password management tools can help to create and enforce complex passwords and keep them up-to-date. This can help to prevent hackers from gaining access to your systems and data.

User Management: Use automation tools to carry out employee onboarding and offboarding processes for any company. Not only do they help to ensure compliance with data regulations, but they also protect both the employee and the company's data. User management technologies can be used during onboarding to automatically identify an employee and grant them the necessary level of access to specific information. In the event that the employee's appointment gets terminated or their user profile becomes vulnerable, the system can easily revoke or suspend their access pending a review.

Event Reporting: Event reporting is the process of documenting and analyzing events that occur within a company's network. This can include everything from malware detections to user logins. Event reporting helps to identify trends and potential issues, and can be used to isolate and investigate incidents. Automated event reporting tools can help streamline the process by collecting data from multiple sources and generating reports automatically. This saves time and resources, and can also help to ensure that reports are accurate and up-to-date. In addition, automated event reporting can help to identify patterns that might otherwise be missed.

7 Raise Security Awareness

One of the most important steps in maintaining data compliance is ensuring that all employees who work with sensitive data understand their responsibilities and use safe practices. This includes not just IT staff but also employees in other departments who may have access to sensitive information.

Education is key to ensuring employees understand the importance of data security and compliance, no matter how it may be inconvenient. They must be aware of the risks associated with mishandling data and the consequences of violating any regulations.

In addition, employees need to know how to protect themselves and the company from potential security threats. This includes knowing how to create strong passwords, how to identify phishing emails, and how to respond to a data breach.

Regular reminders and updates are essential in helping employees stay safe and compliant. It's also important to keep up with regulations and best practices changes so that employees are always up-to-date on the latest security threats.

Ace Your Next Audit with JumpCloud

Any IT admin that wants a smooth audit experience must lay a proper foundation with proven security hygiene measures. Solid foundations yield strong security postures that inspire trust.

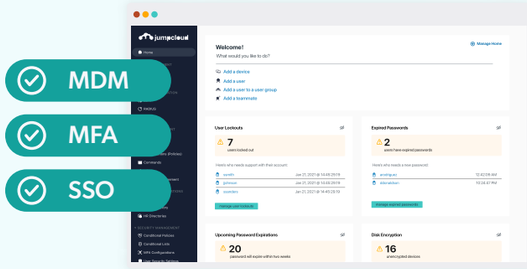
Data compliance hygiene is a valuable asset for any organization when done correctly. A big help in achieving data-compliant status is to employ solutions like the JumpCloud Directory Platform that support data hygienic practices with tool consolidation.

The JumpCloud Directory Platform provides:

- Advanced reporting that gives insight into data access and compliance-related activities
- MFA protocols for logging in to an organization's IT resources
- Effective password policies that comply with best practices
- Device management of all devices authorized to access company resources
- Automation of user onboarding and offboarding

Are you feeling uncertain about how to implement the compliance controls you need? Are you feeling overwhelmed with tool sprawl? If so, the JumpCloud Directory Platform can streamline your security stack and provide real-time audit trails.

Our Professional Services Team can help implement many of the cybersecurity best practices you need to feel prepared come audit time. Hand-off a chunk of your workload to world-class engineers with high-caliber project management skills for a small fee.



The JumpCloud Open Directory Platform™ helps IT teams **Make (Remote) Work Happen**™ by centralizing management of user identities and devices, enabling small and medium-sized enterprises to adopt Zero Trust security models. JumpCloud® has a global user base of more than 180,000 organizations, with more than 5,000 paying customers including Cars.com, GoFundMe, Grab, ClassPass, Uplight, Beyond Finance, and Foursquare. JumpCloud has raised over $400M from world-class investors including Sapphire Ventures, General Atlantic, Sands Capital, Atlassian, and CrowdStrike.

For more information on JumpCloud and how organizations everywhere are providing Secure, Frictionless Access™ to all their IT resources, visit jumpcloud.com/why.

jumpcloud™

Try JumpCloud Free →