COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

A Buyer's Guide to

IT Compliance Management Tools

Introduction

You Can't Comply With What You Don't Know and Can't See

Managing IT compliance in today's ever-growing digital-first world is extremely complex, and companies worldwide find it difficult to implement the many regulations imposed on them. The time-consuming and expensive nature of achieving enterprise-wide compliance makes it challenging, especially for small-medium businesses. It's also important to note that managing IT compliance implies constantly updating an organization's IT security protocols.

Moreover, understanding the controls or requirements set by regulatory authorities, like the Federal Trade Commission (FTC) or General Data Protection Regulation (GDPR), may seem overwhelming, especially considering the deadlines and penalties involved.

It's easy to get lost in a mess of regulatory jargon, risking cyberattacks, hefty fines, reputation and customer loyalty. You can't comply with what you don't know and what you can't see. That's why it's essential to maintain ongoing documentation of your IT compliance efforts to protect yourself by providing the relevant evidence and side-stepping accusations of negligence.

In this buyer's guide, we dive deep into understanding exactly what IT compliance is, why it's important, its relation to cybersecurity, the benefits of compliance management solutions and the key features to look for when purchasing the ideal IT compliance management solution for your organization.

The Purpose of Compliance

IT compliance is about doing everything you are required to do, and doing them right. In many cases, those requirements come from external sources. They can take many forms: federal, state and provincial laws; industry regulations; contractual obligations and insurance requirements.

IT compliance management is essential for organizations, particularly those operating in the finance, healthcare and government industries, where there are specific requirements and standards that must be met to maintain legal and operational integrity. Failure to comply with these regulations can result in severe penalties, legal liabilities, reputational damage and loss of customer trust.

The Health Insurance Portability and Accountability Act (HIPAA) and Defense Federal Acquisition Regulation Supplement (DFARS) are examples of U.S. federal standards that cover the healthcare industry and defense contractors, respectively. Most U.S. states have their own security and data protection laws, like the New York State Department of Financial Services Cybersecurity Regulation, but also data privacy and ethics laws that businesses must follow.

How Does Compliance Fit in Cybersecurity?

The relationship between IT compliance and cybersecurity is complementary. Unfortunately, however, it's a popular opinion that only companies within specially regulated industries, such as financial institutions, need to worry about their cybersecurity practices. The belief is that, for those organizations, data protection is only a requirement for regulatory compliance.

This is far from the truth. Any organization that receives, stores or handles consumer or sensitive business data must always protect that information because it's always at risk. The FTC Safeguards Rule update addresses this very aspect of data management and customer privacy across organizations — even those that do not typically define themselves as financial institutions.

Hackers will never stop searching for the weakest link in your organization's network to gain any level of access. Employees can also pose threats as unintentional or malicious insiders.

In order to safeguard the privacy of your business's intellectual property (IP), employees, partners and customers, regulatory authorities develop and update a slew of security controls that must be strictly implemented. And when you improve your cybersecurity practices and policies, you increase your level of cyber maturity and ability to comply with your respective regulatory authorities.

A Broad Look at Compliance Requirements

IT compliance requirements are those sets of regulations or standards imposed on organizations to align their operations with various legal and ethical business practices stipulated by their respective authorities. Keep in mind that every requirement is subject to change. Organizations must always stay updated on relevant regulations and seek legal advice to establish IT compliance programs tailored to their specific needs for maximum compliance.

Some common areas of compliance requirements are listed below.

Legal Compliance

Encompasses laws and regulations specific to the industry or jurisdiction in which an organization operates. Some examples are data protection and privacy laws, consumer protection laws, labor laws and anti-corruption laws.

Financial Compliance

Organizations must comply with financial regulations to promote transparency, accountability and accurate financial reporting. Tax regulations, anti-money laundering laws and accounting standards fall under this type of compliance requirement.

Data Protection and Privacy Compliance

Here, ensuring compliance entails proper collection, storage, processing and sharing of personal data. Receiving consent from all the relevant parties and individuals is an absolute must.

Information Security Compliance

Adhering to industry-specific security standards, implementing or revising security controls, carrying out regular risk assessments and developing incident response plans are a few basic compliance requirements in this respect.

Corporate Compliance

Organizations must inculcate a culture of following compliance best practices, which include establishing appropriate internal controls, maintaining well-documented and transparent records, conducting audits and ensuring ethical behavior and accountability across every facet of the enterprise.

Types of Compliance

When it comes to managing compliance, there are two main categories: corporate compliance and regulatory compliance. While they both are similar in their function, the main distinction between them is that the former is an internal source of compliance, and the latter is an external source.

01

Corporate Compliance

Corporate compliance is defined as the rules or policies stipulated by an organization to help improve and sustain productivity. It also affects the brand image and quality of service or product delivery.

Regulatory Compliance

Regulatory compliance is a set of requirements imposed by external lawful authorities that seek to regulate a business's operations to keep all its incumbents safe from any liabilities, like cybercrime. Failing to comply will result in severe monetary and reputational repercussions.

02

The Benefits of Using IT Compliance Management Software

No matter where your compliance requirements come from, a well-designed IT compliance management solution can help ensure your security measures are in place and provide evidence of compliance if you are audited, investigated or sued.

IT Compliance management solutions help reduce risks by documenting and enforcing the IT requirements you are supposed to meet. A good compliance management solution will automate and streamline compliance processes, saving your team a lot of time and effort. It provides the documents you need to validate your compliance while enabling you to manage multiple regulatory standards. It can also identify hidden gaps in your network to ensure you remediate them before they become big problems.

The software is designed to centralize compliance-related tasks, like policy creation, training and auditing and features dashboards to monitor and track your IT compliance activities across the enterprise. Maintaining transparency and accountability becomes an extremely simple process. Its automated alerts and notifications allow stakeholders and other relevant professionals to stay updated about upcoming deadlines, regulatory changes and non-compliance issues.

Furthermore, an intuitive IT compliance management solution allows for the implementation of preventive controls, like automated policy enforcement, reducing the likelihood of compliance breaches. It empowers you to easily implement best practices and modify existing standards to create your own that align with your organization's specific IT policies and procedures. It also bolsters your team's compliance incident management capabilities, empowering them to better handle remediation processes. This directly ties in with reducing the level of risk your organization may be exposed to, both from an IT security and compliance perspective.

With many more benefits to offer, an effective IT compliance management solution is also scalable and flexible. It grows in-step with your organization, helping you maintain the highest levels of compliance in today's ever-evolving threat landscape.

Standards and Frameworks

The ideal IT compliance management software is built to help you comply with a wide range of government standards and frameworks, all while possessing the flexibility to establish your own corporate requirement controls. Listed below are some common requirements that IT compliance management solutions must cover.

Standards

- **HIPAA:** Make sure the solution includes this requirement's three Rules: Security, Privacy and Breach Notification. You should be able to track HIPAA and NIST CSF at the same time, even though they have different controls. It would be a bonus if it also covered all required actions for the MIPS Incentive Payment System, and guarantees that your cyber insurance policy pays off in case of a breach.

- **GDPR:** Ensure that the solution supports both UK and EU versions of GDPR. There are distinctions and overlaps between the two, which makes managing them tricky. The solution must feature standard management templates that are designed following its stipulated requirements, including the seven GDPR principles and the eight GDPR individual rights.

- **FTC Safeguards Rule:** This rule seeks to ensure the security and confidentiality of customer information. It was enacted to protect consumers against any anticipated threats to their information and reduce the risk of unauthorized access to, or the use of, such information that could harm or inconvenience customers. The solution should be updated to meet the new requirements mandated by the recent June, 2023, amendments.

- **NIST SP 800-171:** The software must include the Department of Defense (DoD) risk scorecard, System Security Plan (SSP) and Plan of Actions & Milestones (POA&M), all of which are mandatory for DoD contracts. It should be able to automatically score your compliance based on the DoD's specific scoring rules. Since the 800-171 requirements include specific policies and procedures for employees to follow, the ideal piece of software needs to feature an employee portal to help you better track and enforce security awareness training and CMMC policy compliance attestation.

- **CMMC 2.0:** Another requirement set by the DoD, your compliance management tool must include the new Level 1 and Level 2 maturity level standards. It should ideally also feature built-in CMMC 2.0 management templates to assess your readiness for Level 1 or 2 certification quickly. The certification deems a DoD contractor's ability to safeguard sensitive information.

- **PCI DSS:** If you're a merchant or service provider, you must perform PCI DSS self-assessments and report the findings to your merchant bank. Make sure the solution supports every Self-Assessment Questionnaire (SAQ) designated by the PCI DSS. Moreover, it must help you meet all 12 of this standard's requirements for building and maintaining secure networks and systems.

- **Protection of Personal Information Act (POPIA):** Popularly called POPIA, this data and privacy law is a regulatory requirement placed on all businesses by the Republic of South Africa. Your compliance management software should enable users to perform assessments of an organization's implementation of the POPIA requirements associated with Chapter 3 – Part A – Condition 7 – Security Safeguards, sections 19, 20, 21 and 22.

Frameworks

- **CIS CSC v.8:** The Center for Internet Security Critical Security Controls is a comprehensive framework that outlines a set of IT protocols and Safeguards designed to help you improve security posture and mitigate cyberthreats. Make sure your solution is updated and includes all 18 CIS controls and features templates for the three different Implementation Groups (IG), which amount to a total of 153 Safeguards.

- **NIST CSF:** The NIST Cybersecurity Framework provides a broad and well-organized structure that addresses all areas of cybersecurity: Identify, Protect, Detect, Respond and Recover. This particular framework is fully mapped with a voluntary set of guidelines, or security controls, that you can use as a foundation for your IT assessments. Ensure that your compliance management tool includes all the relevant and necessary guidance you'll need to implement each control. It should allow you to customize NIST CSF by either including or excluding specific requirements, and modify existing controls to suit your business operations.

- **Cyber Liability Insurance:** Your solution must enable you to track and manage all your IT compliance and security requirements while making sure your cyber insurance claims aren't denied due to the results of an audit after an incident. Insurance companies will strictly audit your IT security policies, evidence of compliance and a slew of other regulatory criteria to verify whether you've done everything right to the best of your ability. Your solution should not give them a chance to deny your claims.

- **Essential 8:** Compiled by the Australian Cybersecurity Centre (ACSC), the Essential 8 is a set of mitigation strategies you can use as starting points to best circumvent security incidents and improve your cyber resiliency. The eight strategies are designed to safeguard Microsoft Windows-based internet-connected networks. A good compliance management solution will allow you to utilize your existing set of IT assets and security tools to best meet the requirements of the Essential 8.

- **Cyber Essentials and Cyber Essentials Plus:** Your ideal IT compliance management solution will help you meet the requirements of the Cyber Essentials and Cyber Essentials Plus certifications by means of an auditor's checklist. It should enable you to carry out self-assessments of your security program against the controls specified by the UK's National Cyber Security Centre (NCSC), which protects you from about 80% of most basic network breaches.

Key Features of an IT Compliance Management Solution

Listed below are the key features of an ideal IT compliance management solution.

Compliance management templates

- Built-in IT compliance management templates for common standards and frameworks
- Delivers standard-specific reports
- Presents assessment results via consolidated, graphical dashboards
- Tracks common controls across multiple standards

Automated IT compliance documentation

- 360-degree automated data collection
- Dynamic, customized policies & procedures manuals for respective standards
- Automated report generation

Enterprise-class reporting and analytics

- Technical assessment reports
- Technical risk analysis reports
- Technical risk treatment plans
- Plan of Action & Milestones reports (POA&M)
- Auditor's checklists
- Various supporting documents

Employee-related IT GRC tracking

- Role-based task portal for security awareness training and policy documents
- Management access to monitor progress and generate reports
- Employee compliance tracking and reporting

Vendor risk assessment and tracking

- Unique vendor login
- Automated vendor email invite
- Vendor assessment status tracking
- View detailed vendor surveys (Should include historical tracking as well)
- Quick assessments

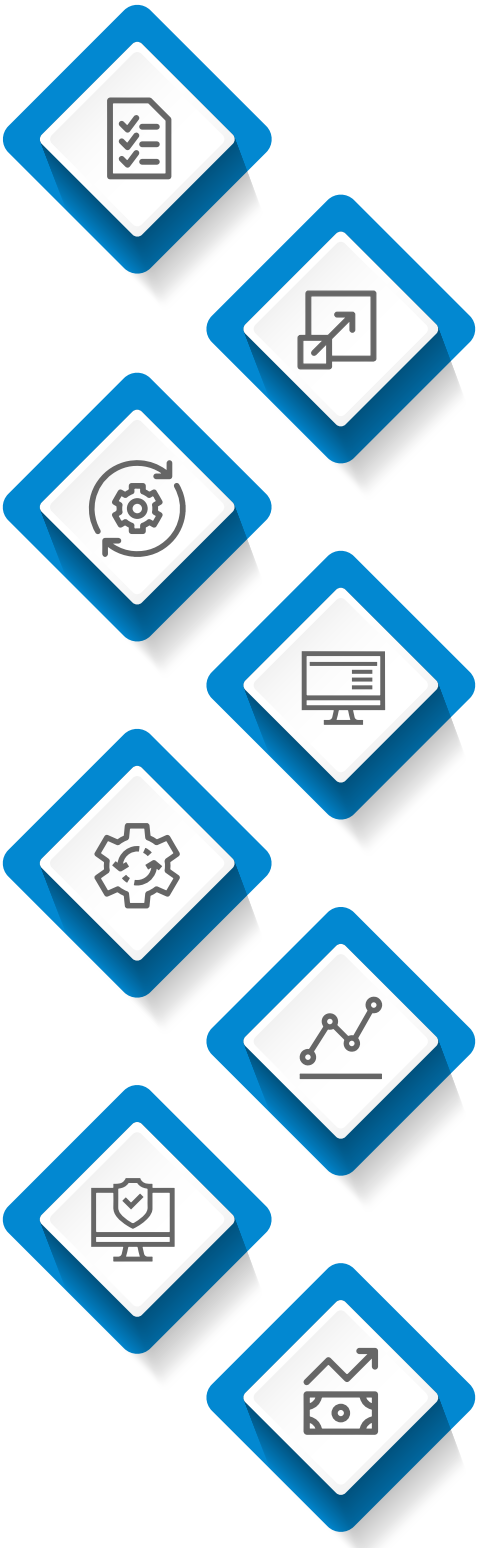
Additional features

- Rapid Baseline Assessments
- Ability to manage multiple compliance standards concurrently
- Role-based architecture
- Customizable libraries of controls, requirements and standards
- Tracks common controls across multiple standards

Factors to Consider When Selecting IT Compliance Management Software

Choosing the perfect compliance management tool to meet your organization's specific needs is easier said than done. You must, in detail, scrutinize every solution based on the following comprehensive list of factors before making a decision. Ensuring that your management and stakeholders actively participate in this critical decision-making process is essential.

Compliance requirements:
Gain a comprehensive understanding of your company's specific compliance requirements and make sure that the solution can properly address them.



Scalability:
Remember that scalability is key in today's world of rapid and continuous evolution of technology and practices. As your organization grows, so does the amount of compliance risks and responsibilities. The solution should be able to grow alongside the business.

Integration capabilities:
The ability to smoothly integrate with your existing systems and IT infrastructure is a very important point to remember. The solution should cohesively work with your environment and cause no disruptions to daily business operations.

Simple UI/UX:
The compliance management tool must be easy-to-use and understandable for all IT professionals. Managing compliance is a very difficult task, and a confusing piece of software creates unnecessary, often risky, situations.

Automation:
Your ideal solution should be able to automate routine tasks, such as policy creation, risk assessments and report generation.

Reporting and analytics:
It must also feature powerful analytical capabilities to gauge compliance performance and generate audit-ready reports. This includes functionalities like real-time analytics and customizable dashboards.

Security:
Managing IT compliance involves handling tons of sensitive data, so ensuring the software is loaded with the necessary security measures, such as data encryption and access controls, is mandatory.

Cost and ROI:
Lastly, consider the solution's ROI. The total cost of ownership, including any additional costs for customization or integration, must be compared against the benefits you derive from it.

IT Compliance Management Solutions Available Today

The market today presents a wide range of IT compliance management solutions that promise to deliver enterprise-class results. Each product varies in terms of sophistication, pricing, number of features, accessibility and overall ease of use. We've reviewed some industry-leading solutions below to help you make the right decision for your organization.

COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

Compliance Manager GRC covers all the bases when it comes to compliance management. It is the first and only purpose-built, role-based IT compliance management platform for both MSPs and IT departments that features automated data collection, a huge database of continuously updated IT controls and requirements, a built-in employee/end-user portal, a dynamic report generator that automatically prepares brandable risk assessments, policies and procedures manuals, plans of action and milestones and a slew of useful supporting documents.

Compliance Manager GRC grants you complete control to edit the built-in controls, requirements and procedures to completely customize your experience. It reduces your risks by taking out the complexity of assuring compliance with your IT security and privacy requirements. And it's priced to be affordable for all, with scalable licensing for both MSPs and IT departments.

Apptega

Apptega focuses on simplifying and streamlining the compliance process. It offers features such as policy and control management, task tracking and reporting. Apptega has a steep learning curve and lacks key risk assessment functionalities that are responsible to help facilitate decision making. Users have also complained about its inefficient UI.

This solution features no automation in data gathering or process flow. They have significant issues in leveraging workflow to document ongoing compliance activities. Its pricing does not justify the takeaways.

TUGBOAT LOGIC
by OneTrust

Tugboat Logic is another cloud-based IT compliance management solutions provider concentrating on risk assessment and compliance automation. The company offers predefined templates and workflows to streamline the IT compliance process. The solution can be complicated for companies that need support with maintaining multiple compliance standards and audits. It has a limited set of features, which create challenges like limitations with evidence collection, compliance tracking, audit management and process automation. TugBoat Logic's product requires a lot of manual intervention to build custom frameworks, leaving much room for error and wasting time in the process.

KnowBe4
Human error. Conquered.

KnowBe4 offers a security awareness and training platform that focuses primarily on cybersecurity and phishing prevention. The KnowBe4 application does not effectively streamline administration of its various modules. Users have expressed frustration with the completeness of training, documentation and onboarding offered. The application's antiquated interface leaves much to be desired. Its email templates are outdated, and several users have expressed a lack of variety. This solution in the list also comes at a high price point.

Summary

In short, IT compliance management software helps organizations comply with their required corporate and regulatory guidelines or frameworks. It assists IT professionals in easily carrying out the responsibilities of tracking, monitoring and auditing their organization's daily IT operations to ensure they conform to all of their IT requirements, regardless of source.

The best IT compliance management software empower organizations to protect their IP, safeguard partner and customer information, create more effective employee training programs and implement the most effective cybersecurity practices.

Moreover, in this buyer's guide, we've touched base on the two types of IT compliance — regulatory and corporate — and their significance to an organization's compliance management practices. Following which, we explained why it's important to adopt compliance management technology in the current digital era. A well-designed solution ensures your security measures are in place and provides evidence of your compliance if you are audited, investigated or sued.

And managing IT compliance would be almost impossible if we didn't know or understand some of today's common compliance requirements and why they were established. We discussed the most important standards and frameworks that currently detail exactly what an organization must do to avoid cyberattacks and protect customer information at all costs.

After reviewing some of the top IT compliance solutions on the market, Compliance Manager GRC stands out to be the solution that offers MSPs and IT departments in small and medium organizations the best value. Considering its comparatively low price point and richness of features found only in enterprise-class alternatives, Compliance Manager GRC is a safe bet for any IT security assurance program.

We hope our comprehensive deep dive into the world of IT compliance has offered some insight into making the right decision when purchasing a compliance management solution.

To learn more about how you can become a master of IT compliance management, visit:
Governance, Risk and Compliance | Compliance Manager GRC