COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

STAY AHEAD IN 2025: YOUR 10-STEP GUIDE TO COMPLIANCE SUCCESS

Are you ready to conquer compliance in 2025? As regulatory requirements tighten, and compliance standards grow more complex, it's critical that businesses maintain a proactive approach to compliance management. This ten-step compliance checklist can help ensure that you are on the right path to achieving your compliance goals in 2025.

THE TRUE COST OF AN INFORMATION SECURITY AND COMPLIANCE PROBLEM

Two-thirds of companies expect an increase in the cost of compliance.[1]

It is 2.7 times more costly not to meet compliance standards.[1]

The average cost of noncompliance has risen more than 45% over the past ten years.[1]

STEP 1. PICK YOUR STANDARD(S)

Choosing the right cybersecurity compliance standard is essential for maintaining compliance, protecting sensitive data and building a resilient security foundation that meets insurance, regulatory and industry-specific requirements.

- ☐ Choose a cybersecurity standard template that aligns with your government or industry requirements, ensuring you're on the right track.
- ☐ Tailor custom standards to meet the specific needs of your cyber-risk insurance policy, business contracts and internal IT policies for seamless governance.
- ☐ Easily manage multiple standards in one place with IT compliance management software, ensuring all your IT requirements are covered efficiently and effectively.

STEP 2. GENERATE THE CYBERSECURITY POLICIES & PROCEDURES MANUAL(S)

Robust IT policies, procedures and documentation are the keys to ensuring that everyone is taking the right actions to maintain security and compliance alignment with regulatory standards.

- [ ] Generate a policy and procedures document for each compliance standard you must meet.
- [ ] Create custom policy and procedures documents for your own standards.

STEP 3. RUN A RAPID BASELINE ASSESSMENT (FIRST TIME ONLY)

Running a baseline cybersecurity assessment is crucial for identifying vulnerabilities, setting a security benchmark and establishing a foundation for ongoing security and compliance.

- [ ] Answer a guided series of questions that directly tie in with the requirements of the cybersecurity standard(s) you have selected.
- [ ] Just answer to the best of your ability, as this is a scoping exercise that will be validated next.
- [ ] You can skip questions that don't apply or that you're unsure about.

STEP 4. PERFORM A FULL TECHNICAL SECURITY ASSESSMENT & CONTROLS ASSESSMENT

Performing a full technical security assessment and controls assessment at the beginning of your process is vital for identifying weaknesses, validating security measures and ensuring a comprehensive, effective strategy for achieving security and compliance.

- [ ] Run automated network and local scanners to gather data on potential issues and risks, aligning them with your standard's controls and requirements.
- [ ] Create easy-to-use interactive worksheets to enhance or validate the data gathered from your IT environment, making the process smoother and more insightful.
- [ ] Upload primary evidence of compliance for any requirements that aren't automatically confirmed through data collection, ensuring a complete and thorough approach.
- [ ] When managing multiple standards, consider running a controls assessment to streamline the IT procedures needed to meet all your requirements simultaneously.

STEP 5. REVIEW THE AUTOMATICALLY GENERATED RISK REPORTS

Reviewing automatically generated risk reports is essential for identifying potential compliance gaps, enabling proactive risk mitigation and ensuring continuous alignment with regulatory requirements.

- [ ] Gather a set of technical assessment reports based on the discovery process.
- [ ] Quantify and prioritize the relative risk of each issue discovered.
- [ ] Generate a ticket in your PSA tool for issues that need immediate attention.

STEP 6. REVIEW YOUR INTERACTIVE PLAN OF ACTIONS & MILESTONES (POA&M)

Reviewing the interactive Plan of Actions & Milestones (POA&M) helps track progress, prioritize remediation efforts and ensure timely completion of tasks, strengthening overall compliance and security posture.

- [ ] Review your Plan of Actions & Milestones, which can be automatically generated by a high-quality solution.
- [ ] Assign individuals or groups to each task and set a due date for the task to be completed.
- [ ] Harness POA&M functions, like a streamlined project management tool, to make sure that all compliance gaps are addressed.

STEP 7. UPLOAD ANY SUPPLEMENTARY EVIDENCE OF COMPLIANCE

Uploading supplementary evidence of compliance is crucial for demonstrating due diligence, supporting audit processes and ensuring a comprehensive and transparent approach to meeting regulatory requirements.

- [ ] An innovative compliance management solution can help you create and log compliance with any requirement through an automated compliance data collection process.
- [ ] This is the time to upload any missing supplementary documents that you have validating that each control is in place and functioning.

STEP 8. ENGAGE YOUR USERS IN MAINTAINING COMPLIANCE

Engaging all your users in compliance is critical to fostering a security-aware culture, ensuring consistent adherence to policies and minimizing human error that could lead to security and compliance risks.

- [ ] Give all end users digital access to all company policies and procedures.
- [ ] Require users to attest to the fact that they have reviewed and agree to them.
- [ ] Provide all end users with regularly refreshed security awareness training that includes phishing simulations.
- [ ] Keep track of who has completed the training and passed a post-training quiz, and who needs more help to minimize human-based risks.

STEP 9. MANAGE YOUR VENDOR RISK

Managing vendor risk is essential to a compliance strategy since third-party vulnerabilities can expose the organization to security breaches and regulatory violations that undermine overall compliance efforts.

- [ ] Talk to your vendors and service providers about their security and compliance procedures.
- [ ] Use a branded, self-serve vendor risk management portal to ensure that your strategic vendors are meeting any IT security requirements you impose on them.
- [ ] Provide each vendor with a separate login and monitor their progress.

STEP 10. RINSE AND REPEAT

Regularly reviewing this compliance checklist ensures that all requirements are consistently met, helps identify potential gaps and supports ongoing adherence to regulatory standards.

- [ ] Perform periodic reassessments and compliance confirmation.
- [ ] Use stored values for previous assessments to determine your current alignment with all of the requisite standards.
- [ ] Generate an Auditor's checklist and identify any changes that may move you out of compliance.
- [ ] Address any new gaps and upload current evidence of compliance.

Maintaining compliance is a complex challenge, and overlooking any aspect of the process can cause an expensive disaster. A solution like Compliance Manager GRC streamlines IT compliance, making it easy for you to track your progress on your compliance journey and pinpoint the actions you need to take to meet any framework or standard.

WHY CHOOSE COMPLIANCE MANAGER GRC?

Compliance Manager GRC is an automated compliance solution that offers unmatched features and benefits.

- Automate your IT compliance process
- Deliver dynamic reports and documentation
- Customize governance and compliance management to your needs
- Provide solid IT security and governance assurance
- Manage compliance requirements for third-party vendors easily

Compliance Manager GRC simplifies the process of compliance with government, insurance, industry and geographic compliance standards. To learn more about how Compliance Manager GRC can help you bolster your security and compliance, request a demo.

REQUEST A DEMO

References:

[1]University of Wisconsin Calculating the Cost of Compliance and Risk.

COMPLIANCE MANAGER GRC™
A Kaseya COMPANY