10-STEP COMPLIANCE CHECKLIST FOR ENHANCED CYBERSECURITY PREPAREDNESS

COMPLIANCE MANAGER GRC™
A Kaseya COMPANY

SMBs are particularly vulnerable to cybercrime, now accounting for 43% of all cyber-attacks. This is due to their limited resources and more casual approach to security, which makes it much easier for hackers to gain unauthorized access.

IT professionals are responsible for protecting the networks they manage and most do their best to follow industry regulations or at least set up their standard security policies and procedures. Yet, lack of compliance with existing security protocols is the leading factor behind most breach events.

THE TRUE COST OF A CYBERATTACK

Cost of cyberattacks – $5 trillion	**Regulatory & compliance fines – $2.3 million**
Reputational damage	**81% of customers stop engaging with brands involved in a data breach**

Our 10-step compliance checklist guide will enhance your cybersecurity preparedness and show you how easy it is to implement any framework or standard using Compliance Manager GRC.

STEP 1. PICK YOUR STANDARD(S)

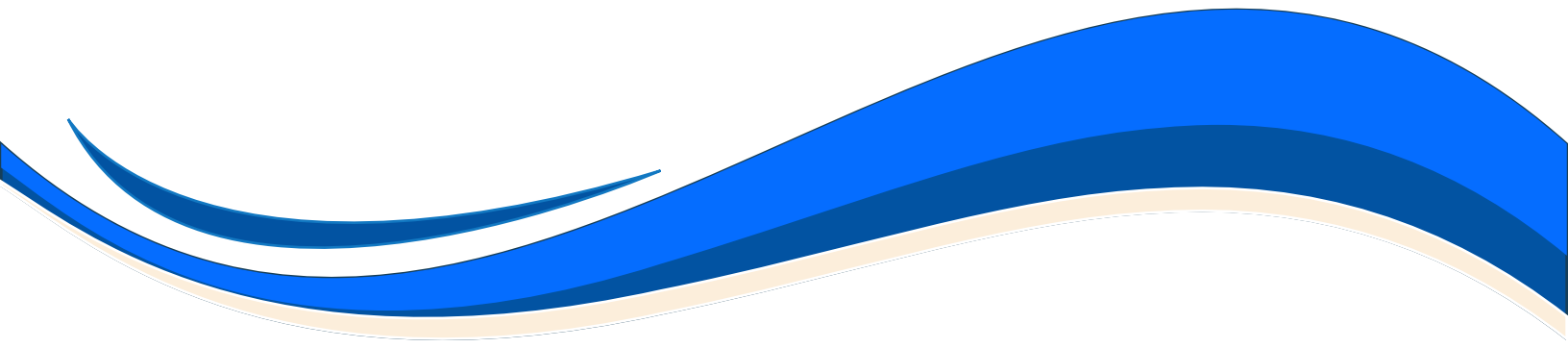
- [ ] Select one of the government or industry cybersecurity standard templates.
- [ ] Create custom standards for your cyber risk insurance policy requirements, other business contractual requirements, and your own internal IT policies and procedures that must be governed.
- [ ] Manage multiple standards to cover all your IT requirements at the same time and in the same place using IT compliance management software.

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

- [ ] Automatically generate a policy and procedures document for each standard.
- [ ] Generate a custom policy and procedures document for your own standards.

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

- [ ] Answer a guided series of questions that directly tie in with the requirements of the cyber security 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

- [ ] Run automated network and local scanners to collect data on issues and risks mapped against your standard's controls and requirements.
- [ ] Generate simple interactive worksheets and complete them to enhance or validate the data collected from the IT environment within your scope.
- [ ] Upload your primary evidence of compliance for requirements that are readily available and not automatically confirmed through the data collection process.
- [ ] If you are managing multiple standards at the same time, you might want to run a Controls Assessment, which combines all of the IT procedures needed to meet all of your requirements at the same time.

STEP 5. REVIEW THE AUTOMATICALLY GENERATED RISK REPORTS

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

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

- [ ] Review the automatically generated Plan of Actions & Milestones.
- [ ] Assign individuals or groups to each task and set a due date for the task to be completed. The 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

- [ ] Create and log compliance with any requirement through CM GRC's 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 EMPLOYEES IN COMPLIANCE

- [ ] Provide all end-users with digital access to all company policies and procedures and require them to attest to the fact that they have reviewed them and agree to them. Record the responses.
- [ ] Provide all end-users with a basic security awareness training course and monitor who has completed the training and passed a post-training quiz.

STEP 9. MANAGE YOUR VENDOR RISK

- [ ] Make sure your strategic vendors are meeting any IT security requirements that you impose on them using a branded, self-serve Vendor Risk Management portal.
- [ ] Provide each vendor with a separate log-in and monitor their progress.

STEP 10. RINSE AND REPEAT

- [ ] Perform periodic reassessments and compliance confirmation.
- [ ] Use stored values for previous assessments for any standard.
- [ ] 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.

This checklist will help you dramatically reduce the risk of a data breach in the event of a cyberattack and avoid fines and lawsuits for non-compliance with government and industry standards.

And, in the event of an unavoidable cyber incident that you could not stop, proving compliance with your cyber insurance policy will guarantee that your claim will be fully paid.

WHAT IS COMPLIANCE MANAGER GRC?

A universal IT compliance management software solution, such as Compliance Manager GRC, is the most efficient way to ensure that ALL your IT requirements are being met, regardless of source. Using the cybersecurity framework templates, you can quickly see how far along you are toward compliance with those standards, and what specific steps you need to take to achieve full compliance.

WHY CHOOSE COMPLIANCE MANAGER GRC?

Deliver IT security assurance aka IT governance

Ensure compliance with government regulations and industry rules

Reduce IT-related risk for you and your clients

To know more about how Compliance Manager GRC can help you stay compliant with regulations, request a demo.

TAKE A DEMO

compliancemanagergrc.com
sales@compliancemanagergrc.com