XM Cyber

Handbook

Plan-Do-Check-Act: 10 Best Practices

to Build a Resilient, Always-On Compliance Program

Bridging the gap between theory and execution is always a challenge - especially in compliance, when requirements usually change faster than internal processes. Adopting a structured approach that combines best practices with the Plan-Do-Check-Act (PDCA) model can help organizations remain agile and resilient in their compliance efforts. The PDCA cycle helps cybersecurity teams get continually better at what they do. When organizations regularly check and update their security measures, they can better protect themselves against new threats and weaknesses.

This handbook demystifies continuous risk management by breaking it down into clear, actionable steps, tailored for security, risk, and compliance leaders. Designed for organizations aiming to integrate compliance into their core operations, this approach moves beyond traditional audit routines. Whether you're navigating NIS2, DORA, SEC rules, or preparing for future compliance challenges, this is your pathway forward.

PLAN Phase

Step 1 - Define the Compliance Objective

- Pinpoint what's driving the compliance effort - a new market, a customer requirement, gaps flagged in a recent audit, or something else
- List the regulations and standards that apply to your business - NIS2, DORA, SEC rules, GDPR, CPPA…
- Be clear about what's at stake if you don't act - revenue, uptime, regulatory pressure, reputational fallout?

Step 2 - Develop a Risk Management Strategy

- Assign clear owners for compliance, security, and operations so responsibilities don't fall through the cracks
- Define what a successful outcome looks like - passing an audit, hitting control coverage targets, reducing response times…
- Choose the frameworks or policies your program will follow, based on your industry, geography, and risk profile

Step 3 - Analyze Current Capabilities

3

- Run a gap assessment to see how your current setup stacks up against what's required
- Spot any blockers early - things like limited staffing, legacy systems, or risky third-party dependencies
- Estimate how much time, effort, and budget it will take to close the gaps
- Flag anything that might not be practical to fix right away and consider phasing it in over time

DO Phase

4

Step 4 - Design and Apply Risk Mitigation Measures

- Determine accepted versus intolerable risks and develop strategies for mitigation and elimination
- Select controls that fit your environment - access restrictions, encryption, monitoring tools, vendor policies, etc.
- Map those controls to the systems, teams, or partners they affect so nothing gets overlooked
- Define how you'll measure whether the controls are working - alerts, metrics, regular testing, or something else

Step 5 - Execute Control Implementation

5

- Put the selected controls in place across systems, environments, and third-party platforms
- Assign owners to each control
- Update infrastructure-as-code, CI/CD pipelines, or IT workflows to enforce compliance automatically
- Let affected teams know what's changing and make sure documentation, runbooks, and internal tools reflect the updates
- Provide targeted training where new processes or approvals are required so teams aren't caught off guard

CHECK Phase

Step 6 - Evaluate Control Deviation Responses

- Set up automated alerts to catch misconfigurations, policy violations, or unexpected changes in system settings
- Define how issues get triaged, who's responsible for fixing them, and how quickly they need to be resolved
- Track remediation in your ticketing or GRC system so nothing falls through the cracks
- Keep a record of what happened and how it was fixed to support audits and internal reviews

ACT Phase

Step 7 - Monitor and Communicate Continuously

- Build dashboards that give execs, security teams, and auditors a clear view of compliance status. The XM Cyber SCM module acts as a single source of truth for the security posture of your entire hybrid infrastructure, to measure and understand the effectiveness of your security controls for comprehensive audit and compliance readiness.

Step 8 - Review and Adapt

- Meet regularly with control owners to review what's working, what's not, and what needs attention
- Adjust controls, roles, or tools when the business or threat landscape changes
- Use monitoring insights to make the case for new investments or to reprioritize efforts

Step 9 - Continuously Measure

- Review key metrics like control pass rates, audit findings, incident trends, and remediation times
- Use tools like breach simulations, red teaming, or automated tests to see if controls are actually working

Step 10 - Look for Ways to Improve

- Flag underperforming controls and adjust or replace them as needed
- Keep compliance evidence current and organized so you're always audit-ready

Building a culture of continuous compliance that prepares you for whatever comes next requires time and effort. However, with the right framework and tools, it becomes achievable, sustainable, and strategically beneficial. Use our Plan-Do-Check-Act (PDCA) compliance handbook in conjunction with the XM Cyber Security Controls Management module to systematically identify, assess, and address security gaps – and ultimately, elevate your cyber resilience.

Want to be prepared for the next compliance requirement on your list?
Check out the XM Cyber Compliance checklists for:

PCI-DSS

NIST 2.0

DORA

XM Cyber is a leader in hybrid cloud exposure management that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia Pacific and Israel.