Checklist: What to Look for in a **Security Compliance Technology Solution**

AUDITBOARD

If you find yourself drowning in a sea of compliance requirements, juggling multiple frameworks, and struggling to keep track of your compliance stakeholders and workflows, it may be time to bring order to the chaos. **The right technology solution can help streamline your InfoSec compliance program in a centralized platform that automates manual processes and enables real-time collaboration and reporting.**

Yet, finding a user-friendly, agile solution that enforces a standard issue management methodology and integrates with other analytics tools is no easy feat. The following checklist contains the most important features you should consider as you search for the right solution for your security compliance program.

Selecting a Security Compliance Technology Solution

The Checklist

☐ **Centralized, single source of truth.**
The risk and regulatory landscapes are constantly evolving and compliance requirements change. As your program matures, juggling multiple frameworks and requirements can become a complex and massive undertaking. A connected platform should facilitate this by serving as the centralized database and single source of truth for your risk, controls, and compliance data. This is foundational because without a proper structural database to support and link different data points to each other, analytics and automation are not possible.

☐ **Automated evidence collection.**
The benefit of a connected platform is that it provides a structured repository of evidence collected. Because your controls are linked to associated frameworks/requirements and risks, it allows your team to collect once, and use many. Having this foundation is essential to automating evidence collection in an efficient matter. Testing workflows should be easily created, scheduled, and repeated so you can integrate with your technology ecosystem and remove the manual effort in collecting evidence. Other features that can optimize the evidence collection process include:

- Automated timestamps when evidence is submitted in the platform.
- Automatic notifications to reviewers when it is time to validate the effectiveness of a control.
- Record of prior year's responses, allowing new team members to understand what was done the previous year.
- Consistent and standardized report formats.
- Real-time reporting, allowing for faster issue identification and longer remediation time.

The Checklist
cont'd

☐ **Real-time collaboration and follow-up.**
A robust InfoSec program requires cross-functional collaboration. Technology should facilitate this through cloud-based features like in-application commenting, tagging, role-based user permissions, automated workflows, and integrations with other collaboration applications, such as Slack and Jira. An example of how this works in action: The InfoSec team can create requests within Jira, directly from the compliance platform, so all questions control owners have can be asked and answered in the tools they already use, which is linked to the security platform itself — with a comments log showing the entire history of the communication.

☐ **Agile reporting capabilities.**
An ideal platform should have configurable reporting capabilities that enable compliance team members to easily create the reports they need — from day-to-day team reporting, quarterly issue reports for executive management, and reports for the CISO to leverage in board meetings. Issues should be automatically reportable anytime they are logged, and status will update in real time as issues move through the remediation process (validated, outstanding, overdue).

☐ **Intuitive and easy to use.**
An ideal technology solution should feel intuitive to its users — from day-to-day compliance team members to process and issue owners, management, and external auditors. An interface should not feel overwhelming to learn and there should not be a tremendous amount of time required to train users. It should feel instinctive in the way it facilitates compliance processes. A solution with these foremost qualities will enable it to scale easily with your InfoSec compliance program as it matures.

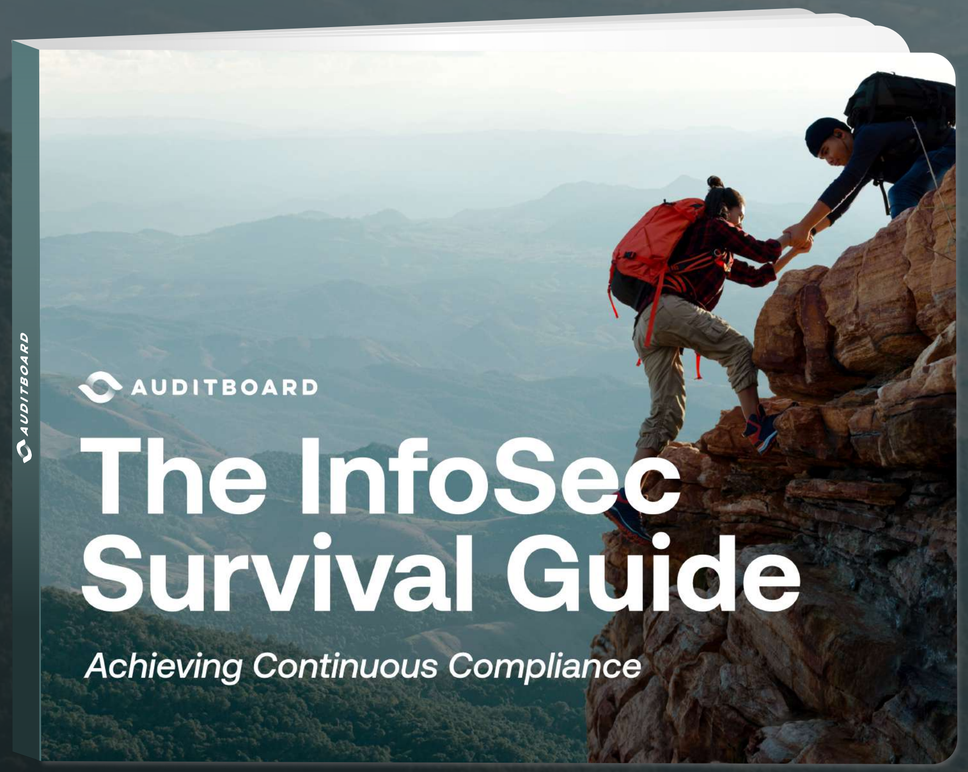
☐ **Issues dashboard that enforces the issues management methodology.**
As mentioned in Chapter 6, a solution should ideally enforce the issues management methodology agreed upon by the business departments that track and manage issues. Your organization-wide issues rating and identification framework should either be applied or formally standardized during implementation, which provides the basis for organization-wide compliance with the standard issues methodology.

The Checklist
cont'd

- [ ] **Standardizing the issues management workflow is essential in maintaining a security compliance program.**
A solution should enforce the issues management methodology agreed upon by key stakeholders throughout the issue management lifecycle. If no formal process is defined, then it is imperative a solution provides the baseline capabilities required to set up and formalize an issue management workflow.

- [ ] **Issue validation workflows that facilitate the issues methodology.**
In addition to enforcing a standardized issues methodology, a solution should also facilitate the issues validation process through automated issue remediation workflows. InfoSec team members can initiate an automated workflow that sends reminder notifications to issue owners with outstanding tasks due.

- [ ] **Ability to integrate with other analytics and workflow tools.**
Once an organization's risk, controls, and compliance data is in a connected platform, a compliance team can use complex queries to join and query the data from different data stores or sources to drive conclusions regarding control effectiveness. There are a number of different applications across an organization's cloud ecosystem that a compliance team might choose to integrate with to accomplish this, such as a data warehouse like Snowflake, or a data analytics tool such as Alteryx.



Get the Full Guide

auditboard.com