riskonnect.

How to Build an Audit-Ready Compliance Program That Grows with You

A compliance program that works over the long haul doesn't chase one regulation after another. That would be impossible considering some industries – like financial services, energy, and healthcare – confront more than 900 regulatory changes per business day.

An enduring and efficient compliance program – that will stand up to an audit – is built around a reusable infrastructure with shared controls, jurisdiction- and regulation-specific tagging, accountable owners, evidence mapping, issue remediation, and regulator-ready reporting.

With the right structure and scalability built into your program, new rules and changing requirements are systematically scanned for, assessed, and folded into the process. Monitoring is automatic. Every action is tracked. Everything is in one place. And every action links back to business objectives.

Identifying your biggest challenges is the first step toward overcoming them. This guide breaks down how to get from tearing out your hair to no-sweat audit readiness. And it isn't hard as you might think.

Your 100-Day Plan

Days 1-25	Days 26-50	Days 51-75	Days 76-100
✔ Build a centralized compliance register – including third parties. ✔ Run a policy audit. ✔ Map controls to required frameworks. ✔ Clarify governance and ownership. ✔ Document regulatory change process.	✔ Revalidate your regulatory scope. ✔ Audit evidence and completion rates to align with requirements. ✔ Run a policy crosswalk to find duplication and conflicts. ✔ Prioritize and score the gap list.	✔ Implement a centralized repository. ✔ Standardize audit trail requirements. ✔ Design reusable "build once, apply many" architecture. ✔ Replace manual monitoring with automation. ✔ Stress-test defensibility before a regulator does.	✔ Redefine success metrics around outcomes, not activity. ✔ Build a cross-domain risk view. ✔ Evaluate technology on interconnection for trust in data. ✔ Use specific regulations as templates for broader resilience. ✔ Provide compliance intelligence for executives and the board.

Step 1: Take Inventory of Your Current Compliance Program

This step is about understanding your current regulatory priorities and program structure.

What regulations are most important to comply with? SOX, the EU AI Act, DORA, ISO 22301, GDPR, HIPAA, FFIEC are a few of the most high-profile obligations, each of which has complex requirements. Which are you following? And what other regulations or certifications are critical because of your industry, location – or because a partner requires it?

What policies do you have in place? Inventory every policy you have, why you have it, what it is intended to cover, and where each is documented.

What controls are in place? Document all controls, the timing, how findings are addressed, and who is responsible.

What is your governance structure? What regulatory frameworks are you following? Map your policies, controls, and documentation to your frameworks for traceability.

What processes do you have for ensuring regulatory compliance? Document your standard operating procedures for assessing risks, conducting a business impact analysis, setting recovery time objectives, submitting evidence, and so forth. Is each regulation or framework handled separately? What is automated and what is handled manually?

What processes do you have for managing regulatory change? Regulatory requirements are updated all the time. Big changes at the federal level are headline news. But there are also lesser-known regional and jurisdictional changes to watch out for. How do you make sure the latest guidance is followed? Who is accountable? Is there a standard process – or is every change handled differently?

Who is ultimately responsible for ensuring compliance obligations are met? Is an owner assigned to every action? Are there other contributors? Detailing accountability will help you understand whether the right people are engaging with the program when they should.

What standards do you require of your vendors and partners? You inherit the risks of your third-party suppliers, as well as their suppliers. What proof are your partners providing to protect you from their misdeeds?

What metrics do you track? Do you use KRIs, KPIs, or some other metric to measure the health of your program?

Step 2: Find the Gaps in Your Compliance Program

This step is about identifying what regulations or requirements you might be missing and what processes don't work as well as they should.

Are you monitoring the right regulations? What was important a few years ago might now be out of date or be meaningless to your business. Are there new regulations or frameworks that you should follow because of changes to your industry, operations, locations, or partner requirements?

What do regulators need to see? Policies are just words without proof that they work. Regulators want to see the evidence. Are you providing all the attestations, controls, documentation, and other evidence to prove compliance to regulators and prevent errors? Simply tracking completion rates is not enough.

How effective are your policies, processes, and controls? Are your controls meaningful? Are you regularly testing and reviewing evidence that your policies, processes, and controls are effective? Are deficiencies being addressed? Can you prove effectiveness to regulators, partners, and your board – or are you wasting time on things that don't matter?

Is there overlap between policies, regulations, or controls? Consider the amount of cross-walking between regulations, controls, and policies. When policies are created in response to a specific event like a new regulation, for example, you can easily end up with multiple policies on the same thing. Are your policies out of sync with current needs? This is the time to clean up your policy library and eliminate duplication and conflicts. Note that having overlapping policies does not necessarily mean you don't have a giant gap somewhere else.

Are you effectively remediating problems? Every organization has failed controls. Regulators want to see not just that you identified the problem, but that you fixed it. Does a failed control kick off a remediation workflow? Is there an audit trail for validating the fix? Are you capturing the right evidence? Are there downstream or upstream effects? Are there gaps with third parties?

Are the right people involved? Compliance cannot be the responsibility of any one department, be it legal, IT, business continuity, or risk management. Have any stakeholders been left out of the process? Are there gaps in the flow of communication?

Have you missed any important regulatory updates in the past? Monetary fines for noncompliance are at an all-time high. And the reputational hit can be just as damaging. If an auditor discovers your policy is based on requirements five years out of date, you are going to be in trouble. How do you prevent that from happening?

Is your compliance program evolving? Your organization, operations, and regulatory landscape can change over time. How do you ensure your compliance program keeps up? And how do you close the gaps?

Step 3: Make Yourself Defensible

This step is about bringing your process, documentation, and proof together to withstand external scrutiny.

Centralize documentation. Having all compliance-related items in a single repository with robust tracking capabilities helps you connect policies, procedures, controls, and regulations, identify redundancies, and plug any gaps.

Clarify your audit trail. Document every compliance action in context of your policies, assessments, controls, remediations, and incident response, so you know who did what when.

Build architecture that scales. Construct a repeatable process for ingesting, analyzing, and operationalizing new requirements. Instead of reinventing the wheel every time, you can leverage a single action – like a policy or an assessment – across multiple mandates. This reduces the amount of time and effort from the compliance team, while establishing consistency and assuring quality throughout the program.

Automate monitoring and enforcement. Use technology to continuously scan for regulatory updates, test controls, flag anomalies, and remediate issues. You'll always have an up-to-the-minute look at what is happening instead of relying on the snapshot-in-time view offered by periodic reports.

Use AI. Delegate some of the busy, but important, work to AI. No organization has the labor force to analyze thousands of policies, for instance. AI can search SharePoint for all policies that relate to NIST2, AI governance as it relates to the EU AI Act, or by jurisdiction. AI can also identify regulations that are out of date and review evidence that your controls are effective.

Remove communication obstacles. Interconnected technology that is accessible to all stakeholders ensures everyone works with the same set of facts. A seamless data flow also makes it easier to exchange ideas, make universal improvements, and capitalize on the good work one group is doing. A single system of record is ideal, but multiple systems can work as long as you have the right connectors.

Cut the waste. Eliminate obsolete policies, controls, and processes that don't tie to a current regulation, requirement, or corporate priority.

Reclaim Your Sanity

Software cuts audit prep time by as much as 80% – and virtually eliminates errors. That's about 3,000 hours per year you can redirect to other work.

Step 4: Link Compliance Back to Operations, the Enterprise, and Business Goals

This step is about meaningfully connecting your compliance program to improve the business.

Focus on outcomes. Simply checking boxes doesn't cut it anymore. A well-constructed compliance program provides the infrastructure to handle operational disruptions, protect against data breaches, cope with third-party failures, avoid fines and penalties, and get back to generating revenue.

Stop focusing on features. Don't get so fixated on a menu of software features that you miss the big picture. The real power comes from interconnection. An unobstructed view of your entire program gives you context. You can see how a single risk might flow through enterprise risk, third-party risk, compliance, internal audit, and IT – and how it might impact corporate performance. That visibility is what leads to better decisions.

Deliver decision-making intelligence. Use what is required by regulators to improve the business. Embed resilience plans in enterprise risk. Start with DORA requirements to improve the overall resilience of your organization. Apply the EU AI Act to establish guardrails around AI use that strengthen trustworthiness. Articulate outcomes in a way that executives, boards, and regulators can understand – and turn that intelligence into action.

Break the Cycle of Chasing Regulations – Once and For All

Regulations will keep changing. Business conditions will keep shifting. New risks will keep emerging. The only way to keep up is to build a compliance program with an adaptable, scalable, reliable structure.

That starts with the fundamentals: know what you have, find what's missing, document what works, and connect every action back to the business. From there, technology can help you scale the process by leveraging controls over multiple mandates, identifying redundancies, holding internal and external stakeholders accountable, and keeping evidence organized and accessible.

Technology is the backbone of an efficient, scalable compliance program. It is the aggregator of information that gives you speed and consistency, without sacrificing trust or accuracy. Regulatory reporting is a breeze. And you can answer even the toughest questions from auditors, regulators, and the board.

You'll have a compliance program that is easy to manage, easy to defend, and easy to adapt. Instead of scrambling to figure out what to do with every new regulation, you can focus on improving effectiveness, strengthening resilience, and helping the business make better decisions. And you'll never again have to worry that something critical will slip through the cracks.

Start building your audit-hardened program here. For more on Riskonnect, please visit riskonnect.com.

Five Questions to Ask About Compliance Software

1	**How easy is the technology to use?**	Riskonnect is easy for even occasional users to master.
2	**Does the software easily integrate with other systems?**	Riskonnect seamlessly integrates with other risk functions – enterprise risk, third-party risk, IT risk, internal audit, etc. – as well as HR, finance, and other parts of the business.
3	**Does the software have built-in AI capabilities?**	Riskonnect has integrated AI, purpose-built to understand the complexities of interconnected risk in context of the organization, its values, priorities, and market conditions.
4	**How secure is the system?**	Riskonnect offers the highest end-to-end security that has been independently certified.
5	**How easy is it to make changes?**	Riskonnect is easy to modify for changing requirements and priorities without the help of IT or the software vendor.

Start anywhere. Expand everywhere.

Riskonnect is the leading provider of software that brings risk under one roof. The technology empowers organizations to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific.
To learn more, visit riskonnect.com.

INSURABLE RISK | GOVERNANCE, RISK & COMPLIANCE | BUSINESS CONTINUITY & RESILIENCE

CONNECT NOW

riskonnect.

08.26