Diligent Compliance

How to Measure and Automate Compliance in 2021

Including a Complete Compliance Automation Maturity Framework

— Where does your business stand?
— What's holding it back?
— What can you gain from automation?

The Compliance Health Check

When we don't feel well, our family doctor is normally the first place we go for help – right after another COVID test, at least. But looking after people's physical and psychological wellbeing takes a network of specialist health professionals, particularly in the face of a pandemic. Only by working together can they provide effective treatments. Understanding how to navigate this system, when to seek extra support, and where to find it are crucial for health workers.

Compliance professionals share similar needs. Today, the growth of restrictions, regulations, and policies is nothing short of wild. In 2020, over 50 countries launched privacy regulations. Since 2011, the cost of non-compliance has risen by 45%. The rising economic cost of red tape in Australia alone is at least $176 billion a year – the equivalent of $19,300 per household – according to the Institute of Public Affairs.

While the government is determined to lessen the regulatory burden, the pressure on compliance teams is only going up as their field of responsibility gets bigger.

The universe of risks is continually expanding with organisations playing catch up to customers' growing social and environmental demands. Digital strategies have amplified data and technology risk. Public tolerance for poor corporate conduct is at a low.

Boards are leaning more heavily on compliance teams as they take an increasingly active role to keep the business safe. At the same time, resources are thinly stretched as organisations recover from COVID's economic impact. The right application of technology can go a long way to help compliance professionals meet these challenges.

This guide will demonstrate that compliance automation is necessary, desirable, and practical. To make these ideas immediately useful, we provide a maturity framework to help teams and leaders assess their current compliance program and understand precisely where automation can be most helpful.

Diligent
Compliance

CONTENTS

Diligent
Compliance

Chapter 1.
To Survive: Automate

To manage the sharp increase in compliance complexity, leading teams are turning to software. One of the advantages algorithms provide is they excel at quickly parsing large volumes of structured data such as regulatory codes. Computers are also tireless. Provide computers with the right inputs, and a computer system can relieve a compliance manager of routine tasks like check-ins or decomposing gaps into action plans so they can focus on higher order business.

Compliance teams aided by automation more quickly achieve:

- Objectivity: In such a fast-paced environment, teams can't and shouldn't trust themselves to remain objective. Internal audits are notoriously unforgiving and without a clear baseline or context, it's difficult to maintain compliance across many realms — especially ones where auditors aren't experts.

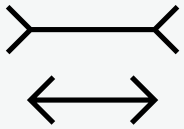
- Trust: With the move to the cloud and the increase in cyber-security breaches, all organisations are to some degree, vulnerable. Partners now demand strict compliance with automation and an easy way to maintain standards to prove it.

However, before you go evaluating compliance automation software, you'll need a plan and process. Otherwise, you may not get nearly as much out of it as you would have otherwise.

Computers can compensate for quirks in human reasoning

Our brains are good at many things. Thinking logically is not always one of them. Our minds are invisibly influenced by cognitive biases, which is why we consistently set unrealistic deadlines or assume others know what we know. Being aware of these biases doesn't always protect us. In the example pictured, even after you measure the lines, your brain will continue to entertain the illusion.

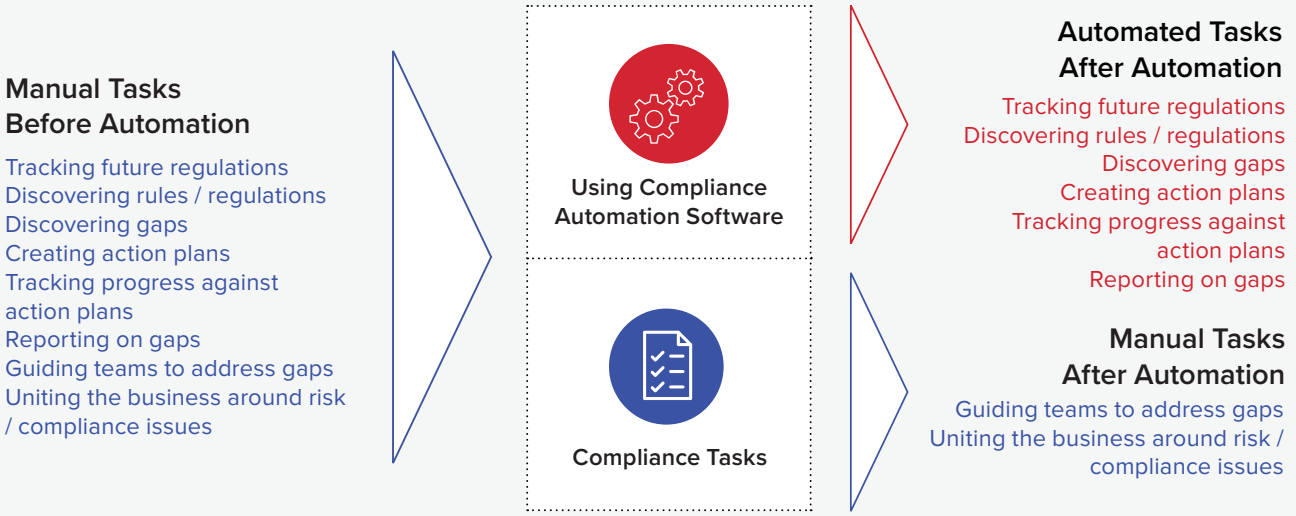
Q: Which line is longest?



A: They're identical

Diligent
Compliance

Compliance automation software reduces the span of control to a manageable level



The Compliance Automation Maturity Framework

Every year, thousands of companies purchase software they never use. In the software industry, it's called shelfware. Why might a company pay for a software system it never actually boots up? Almost always, it's because it jumped the gun and invested in technology without an accompanying process. Before you can reduce your workload with automation, you must understand what you want it to do, and implement with that goal in mind.

To this end, we've developed the Compliance Automation Maturity Framework (hereafter, the Maturity Framework). It's an assessment to give you everything you need to understand where your business stands today. By that virtue, it presents you with a list of recommendations for climbing to higher and higher levels of compliance automation maturity.

How does the assessment work? The higher your business climbs on this chart, the greater the compounding efficiencies. For example, compliance automation software applied to a business that doesn't yet know what it must comply with (or why) may help it discover and track liabilities.

But the software will be far more useful to a company with a well-supported and clearly-defined compliance program. The latter sort of company will be able to automate routine tasks. They'll not only discover gaps, but also automatically decompose them into action plans that are then assigned and tracked.

How the framework works:

There are five levels of maturity that exist on a spectrum of compliance maturity, which we define as a business that's able to manage its risk, reduce its administrative burden, and continuously improve. The higher on the framework, the greater the lower the risk and relative cost.

There are five attributes for each level:

- **Questions:** The prevailing question the compliance team is asking
- **Measurement:** How the team measures compliance
- **Awareness:** The internal awareness and perceived importance of compliance
- **Security:** Level of cyber-security awareness and actions required
- **To Improve:** Actions that will increase maturity

Benefits of the framework

The Maturity Framework is designed to save companies from some of the most pernicious problems that afflict compliance teams and programs:

Uninformed decisions

Without benchmarks or context, compliance teams can believe they're covered when they are not. Or, they can be pleasantly unaware of regulations that affect them. Teams that make decisions without a baseline risk straying further and further into non-compliance.

Often, leaders of companies with poorly defined or poorly-supported compliance teams trust that things are being managed when they are not. They inaccurately assume, like insurance buyers who haven't yet experienced an earthquake, that an absence of evidence is evidence of absence.

The time / budget trap

Under-resourced compliance teams often begin with lofty expectations and settle for minor adjustments. The reason is often a deficiency in time or resources. If executives haven't experienced issues like audits or fines, it's difficult for them to appreciate the scope of the problem and budget accordingly.

Impenetrable silos

Left to their own devices; risk, compliance, and quality assurance teams will each develop their own approaches and frameworks. This leads to both gaps and wasteful overlaps. It's also common for cyber-security to be treated as a separate function when it is in fact highly interrelated. Among manufacturers, for example, the CTO often does not also own security for the shop floor, where machines are increasingly wired to the internet. And within healthcare and finance, 90% of breaches begin with a human error like clicking a link in a phishing email.

Wrong tools and tech

When it comes to technology, the compliance space is still an immature market. A majority of compliance managers rely on ad-hoc systems like spreadsheets that lack the integrated awareness that comes with a real software platform. Often, spreadsheets create a paper trail, but at the cost of valuable time, and sometimes, simply create more work.

Diligent
Compliance

The Compliance Maturity Framework

From

Unknown risk → Manageable risk
High administrative burden → Low administrative burden
Suffers from entropy → Benefits from entropy
Future shock → Future proof
Reactive team → Proactive team

Attributes	Level 1 Performed/Initial	Level 2 Repeatable/ Managed	Level 3 Defined/ Established	Level 4 Predictable/ Measured	Level 5 Optimised
Questions	How to perform initial compliance scan? How the process aligns with minimum best practice requirements?	How can repeatable compliance tests help? How well the process aligns with process specific management?	What insights can we gain from the risks? How the processes satisfy specific work product, quality and performance outcomes?	How can we use our data to predict issues and intervene early? How can organisations demonstrate an ability to control and manage its processes?	How can we use our data to predict issues and intervene early? How can organisations demonstrate an ability to control and manage its processes?
Measurement	Process Performance Basic benchmarks High-level scan General Practices Basic compliance and risk assessments	Work Product Management & Performance Management Some benchmarks Minimum Best Practice General Practices with Process Specific Practices Measures compliance and risk using software but still largely reliant on manual effort	Process Deployment & Process Definition Industry-specific benchmarks Minimum Best Practice Performance & Reporting Measures compliance and risk using a software solution that also allows users to set goals and measure progress	Process Control & Process Measurement Verified, industry-specific benchmarks Full Process Assessment Performance & Reporting Reporting of gaps that are translated into actionable plans and tasks Reporting on compliance gaps, initiatives, actions, and progress	Process Innovation & Process Optimisation Verified, industry-specific benchmarks Full Process Optimisation Continual Improvement Tracking to include wide range of compliance requirements from ISO standards to data privacy. Reporting on compliance gaps, initiatives, actions, and progress

The Compliance Maturity Framework (Continued)

Attributes	Level 1 Performed/Initial	Level 2 Repeatable/ Managed	Level 3 Defined/ Established	Level 4 Predictable/ Measured	Level 5 Optimised
Awareness	Performed but not standardised or formally managed Some or low awareness of compliance Some internal audit program, or a mostly toothless program	Consistent performance and work product outputs Moderate compliance program Internal audit program	Documented, deployed and consistently followed Established compliance program with executive-buy in Compliance goals are aligned with business goals Internal and external audits adaptive to the organisation with appropriate actions	Fully managed, integrated, measured, and controlled Clear cross-departmental cooperation and coordination; everyone is on-board and aware of where they fit into the risk-management hierarchy Centralised repository for control documents to prevent divergent versions Mature internal and external audit programs with appropriate actions	Able to meet current and projected business goals Clear cross-departmental cooperation and coordination; everyone is on-board and aware of where they fit into the risk-management hierarchy Teams are responsible for tasks, goals, and progress Centralised repository for control documents to prevent divergent versions Advanced internal and external audit programs with appropriate actions
Security	Some or low adoption of security measures Basic or sporadic security testing (stress tests, penetration testing, etc.) Some business disaster or continuity planning	Adoption of a cyber-security control framework (ISO, NIST, COBIT) Some security testing (stress tests, penetration testing, etc.) Basic business disaster or continuity plan	Mature internal cyber-security control framework Disaster recovery and business continuity plan Intermediate stress, vulnerability, penetration, and red-teaming tests Moderate business disaster or continuity plan	Mature internal cyber-security control framework Proven disaster recovery and business continuity plan Thorough stress, vulnerability, penetration, and red-teaming tests Advanced business disaster or continuity plan	Optimised internal cyber-security control framework Innovative disaster recovery and business continuity plan Thorough stress, vulnerability, penetration, and red-teaming tests Innovative business disaster or continuity plan

The Compliance Maturity Framework (Continued)

Attributes	Level 1 Performed/Initial	Level 2 Repeatable/ Managed	Level 3 Defined/ Established	Level 4 Predictable/ Measured	Level 5 Optimised
To Improve	Obtain objective benchmarks Adopt a risk management framework Adopt software to discover and track regulations and governance Adopt consistent performance and work product outputs	Obtain industry-specific benchmarks Make compliance performance and work product outputs consistent Adopt a more mature cyber-security framework Adopt compliance software to identify gaps, decompose risks into action plans, and track	Obtain verified industry-specific benchmarks Document, deploy and consistently follow compliance program Onboard the company onto a compliance software where teams manage their own action plans, automate tasks, and there's a centralised repository Begin cross-departmental coordination with help of C-Suite and board	Develop compliance team soft skills Fully manage, integrate, measure, and control compliance objectives Enhance compliance software usage where teams manage their action plans, automate tasks, and there's a centralised repository Increase cross-departmental coordination with help of C-Suite and board Engage in advanced cyber-security tests; war-game disaster recovery and business continuity plan	Enhance compliance team soft skills Continue to innovate as the business advances with compliance goals Increase cross-departmental coordination with help of C-Suite and board for longterm compliance planning and execution Maintain cross-departmental coordination with help of C-Suite and board Perform "next-generation" cyber-security tests; war-game disaster recovery and business continuity plan

Diligent
Compliance

Chapter 2. How To Implement the Framework

To implement the framework, take your team through six questions. While they are deceptively short, they will take time to work through as a business. It is best to assemble a strike team of willing advocates from the compliance, risk, quality assurance, IT, and legal teams to address them, and it must begin at the top. It is a rare organisation that ascends the Maturity Framework without unconditional executive support.

1. STRATEGY

What is the vision?
First, lay out the vision for what you hope to achieve. In this ideation session, there are no bad ideas and no need to assess the realism of the vision — only to develop something that fully addresses all the company's present and future issues. (The realistic assessment comes later.)

Condense that vision as much as possible — perhaps into as few as 2 - 6 principles for your program. These principles are your North Star, and all compliance efforts should align to them. Then, decompose these principles into workflows.

- What tasks and roles are necessary to achieve them?
- What would have to come true for you to reach the vision?

Record the results and set aside.

2. BASELINE

Where are we now?
Conduct a risk-based assessment and determine how you're going to measure success toward your tasks, workflows, and vision. It can be helpful to look at baselines — and better yet, industry-relevant baselines. Identify the specific metrics, their data sources, and even if potential future sources not currently a reality. (This can serve as a roadmap to greater compliance maturity.)

- Based on all of this, where is your effort most useful?
- Where should you begin?

3. ANALYSIS

Where do we want/need to be?
Consult the Maturity Framework. Where is your organisation today? If your organisation's efforts seem scattered throughout maturity levels, select the level where the greatest number of attributes align, and note where particular attributes fall behind. For instance, you can be at Level 2, but have a cyber-security program that's at Level 1.

Attributes	Level 1 Performed/ Initial	Level 2 Repeatable/ Managed	Level 3 Defined/ Established	Level 4 Predictable/ Measured	Level 5 Optimised
Measurement		✖			
Awareness		✖			
Security	✖ Cyber Security Concerns				
To Improve		✖			

- Based on your current level of compliance maturity, what is necessary to move to the next level? Record these in extensive detail to serve as a basis for planning.

Diligent
Compliance

4. PLANNING

How do we get there?
This is where you begin to involve other teams and more members of your own team. Determine how will you resource this project and ideally, enlist executive and board-level support in doing so. Identify the measurement, frequency, and methods of capture, and enlist operations needed to put that into place. Now, conduct an automation assessment:

Given your current access to technology, what tasks can be reasonably automated to make your organisation's compliance to the framework more manageable?

If you plan to evaluate new software, begin the evaluation early, and ask vendors for information on what challenges similar organisations are running into, how they are solving them with software. Use this information to build your evaluation criteria.

The Compliance Maturity Framework

Attributes	Level 2: Repeatable/Managed
Questions	What don't we know? How can compliance help the business?
Measurement	Some benchmarks Measures compliance and risk using software but still largely reliant on manual effort
Security	Adoption of a cyber-security control framework (ISO, NIST, COBIT)
To Improve	Obtain industry-specific benchmarks Align compliance goals with business goals Grow internal audit program to adapt to different business units Adopt more mature cyber-security framework Adopt software to identify gaps, decompose risks into action plans, and track

5. MEASUREMENT

How do we know we've arrived?
Track progress and improvement toward your metrics, tasks, workflows, and vision. Address data quality issues and reevaluate the technology stack that supports it all.

- Is the system functioning as desired?
- Can it be changed or are there reasons to enter into a new evaluation?

6. PLANNING

How do we keep the momentum going?
In this ongoing phase, train the company and encourage a security-minded culture. Process and technology are vital, but without cultural compliance, the program can still fail. At this stage, it can help to train your compliance and risk teams on soft skills so they're not just spreading the right message, but making sure that message is persuasive with your staff and employees.

Review your original vision. If necessary, update it.

- Does your program stand a reasonable chance of achieving framework compliance?
- If not, what can you adjust?

Assess, decide, and repeat.

Diligent
Compliance

The Journey Begins

The need for compliance automation has never been greater. Like the once-mighty master builder, the all-knowing compliance manager of yesteryear is being phased out. In their place, companies are confronted with a choice: Either hire enough people to assess and control risk against standards from thousands of regulatory bodies and expanding internal governance or, more plausibly, turn to software.

Compliance automation systems can vastly improve the efficacy of compliance teams and are quickly becoming the standard. With them, small teams can have a big impact, and can be more objective and instill more trust in partners. They can effortlessly scan and adapt to emerging regulations, identify gaps, and by virtue of having less administrative work, spend more time uniting the company and making a case for true, complete compliance.

If the Maturity Framework is the start of your journey, automation software is the vehicle that helps you reach the objective with ease. After all why walk when you can drive? But the real hurdle is enlisting complete executive support because it's a journey with a fluid destination. Regulations will continue to change. Governance will continue to change. And business will continue to change. Your best hope is to simply move closer and closer to a way of doing business where risks are low, known, and addressed as a byproduct of doing business.

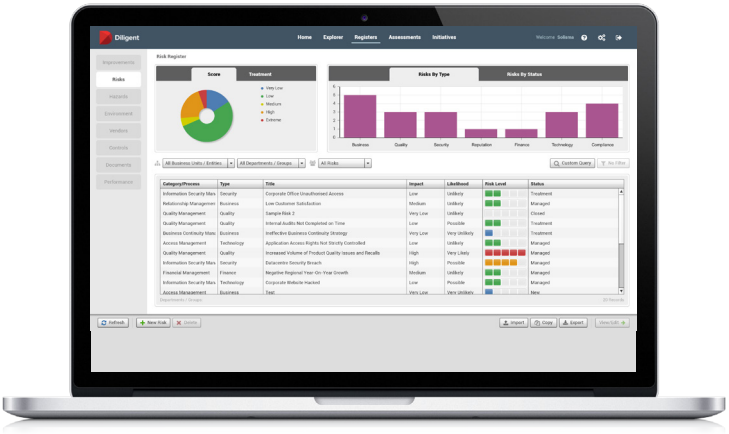
"The cost of non-compliance is 2.71 times higher than cost of compliance."

Ponemon

Diligent
Compliance

What is Diligent Compliance?

Diligent Compliance helps companies manage their compliance with both internal and external obligations, identifies gaps, and suggests remedial tasks that will help drive continual improvement and business continuity.



- Dashboards and reports for visualising program effectiveness
- A central library of internal frameworks and obligations
- Common controls that dynamically map related obligations
- Discover gaps and assign actions
- Track and report on progress

Learn more at:
learn.diligent.com/compliance-anz